aws

Référence de l'autorisation de service

Référence de l'autorisation de service

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Référence de l'autorisation de service: Référence de l'autorisation de service

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Référence 1
Actions, ressources et clés de condition 1
Tableau Actions 1
Tableau Types de ressources 2
Tableau Clés de condition 3
AWS Gestion du compte 19
AWS Recommandations d'action 26
AWS Activez 28
Opération d’IA Amazon 32
Alexa for Business 47
AmazonMediaImport 66
AWS Amplifier 69
AWS Amplify Admin 79
AWS Générateur d'interface utilisateur Amplify 89
Apache Kafka APIs pour les clusters Amazon MSK 103
Amazon API Gateway 111
AWS App Mesh 114
AWS Aperçu de App Mesh 127
AWS App Runner 136
AWS Studio d'applications 153
AWS Conteneur App2 157
AWS AppConfig 160
AWS AppFabric 176
Amazon AppFlow 187
Amazon AppIntegrations 196
AWS Application Auto Scaling 213
Application Discovery Arsenal 222
AWS Application Discovery Service 225
AWS Service de migration d'applications 239
Amazon Application Recovery Controller – Changement de zone 317
AWS Service de transformation des applications 329
Amazon AppStream 2.0 333
AWS AppSync 359
Commutateur de région Amazon ARC 378

AWS Artifact 385
Amazon Athena 390
AWS Audit Manager 409
Amazon Aurora DSQL 424
AWS Auto Scaling 431
AWS Échange de données B2B 434
AWS Backup 442
AWS Passerelle de sauvegarde 468
AWS Backup Search 475
AWS Stockage de sauvegarde 480
AWS Batch 485
Amazon Bedrock 505
Amazon Bedrock AgentCore 568
Amazon Bedrock propulsé par AWS Mantle 609
AWS Billing 623
AWS Billing et tableaux de bord de gestion des coûts 632
AWS Billing Et exportations de données de gestion des coûts 636
AWS Billing Et calculateur de prix pour la gestion des coûts 642
AWS Billing Et actions recommandées en matière de gestion des coûts 651
AWS Billing Conductor 654
AWS Billing Console 664
Amazon Braket 668
AWS Service du budget 675
AWS BugBust 681
AWS Certificate Manager 690
AWS Chatbot 697
Amazon Chime 708
Claude Platform sur AWS 781
AWS Chambres propres 788
AWS Clean Rooms ML 826
AWS Cloud API de contrôle 851
Amazon Cloud Directory 854
AWS Cloud Carte 869
AWS Cloud9 880
AWS CloudFormation 891
Amazon CloudFront 921

Amazon CloudFront KeyValueStore 954
AWS CloudHSM 957
Amazon CloudSearch 968
AWS CloudShell 974
AWS CloudTrail 979
AWS CloudTrail Données 1001
Amazon CloudWatch 1004
Informations sur les CloudWatch applications Amazon 1021
Signaux CloudWatch d'application Amazon 1028
Amazon, CloudWatch évidemment 1034
Amazon CloudWatch Internet Monitor 1043
Amazon CloudWatch Logs 1049
Moniteur synthétique Amazon CloudWatch Network 1077
Gestionnaire d'accès Amazon CloudWatch Observability 1082
Service d'administration Amazon CloudWatch Observability 1088
AWS CloudWatch RHUM 1102
Amazon CloudWatch Synthetics 1108
AWS CodeArtifact 1117
Amazon CodeCatalyst 1129
AWS CodeCommit 1140
AWS CodeConnections 1162
AWS CodeDeploy 1176
AWS CodeDeploy service de commandes hôte sécurisé 1189
Amazon CodeGuru 1192
Amazon CodeGuru Profiler 1194
CodeGuru Réviseur Amazon 1201
Amazon CodeGuru Security 1209
AWS CodePipeline 1214
AWS CodeStar 1226
AWS CodeStar Connexions 1233
AWS CodeStar Notifications 1249
Amazon CodeWhisperer 1259
Amazon Cognito Identity 1266
Amazon Cognito Sync 1277
Amazon Cognito User Pools 1283
Amazon Comprehend 1305

Amazon Comprehend Medical 1342
AWS Compute Optimizer 1349
AWS Automatisation de Compute Optimizer 1361
AWS Config 1368
Amazon Connect Cases 1398
Amazon Connect Customer Profiles 1409
Amazon Connect Health 1434
Campagnes sortantes Amazon Connect 1445
Amazon Connect Voice ID 1453
AWS Service de connecteurs 1460
AWS Management Console Appli mobile 1463
AWS Facturation consolidée 1466
AWS Catalogue de contrôle 1468
AWS Control Tower 1472
AWS Rapport sur les coûts et l'utilisation 1487
AWS Service Cost Explorer 1492
AWS Hub d'optimisation des coûts 1509
AWS Service de vérification des clients 1512
AWS Data Exchange 1515
Amazon Data Lifecycle Manager 1527
AWS Data Pipeline 1532
AWS Service de Migration de Base de Données 1543
Database Query Metadata Service 1581
AWS DataSync 1585
Amazon DataZone 1602
AWS Deadline Cloud 1635
Amazon Detective 1677
AWS Device Farm 1687
AWS DevOps Service d'agent 1708
Amazon DevOps Guru 1721
AWS Outils de diagnostic 1729
AWS Direct Connect 1734
AWS Service de répertoire 1751
AWS Données du service de répertoire 1783
Clusters Amazon DocumentDB Elastic 1794
Amazon DynamoDB 1816

Amazon DynamoDB Accelerator (DAX) 1844
Amazon EC2 Auto Scaling 1852
Amazon EC2 Image Builder 1884
Amazon EC2 Instance Connect 1921
Service MCP Amazon ECS 1926
Amazon EKS Auth 1928
Serveur Amazon EKS MCP 1931
AWS Elastic Beanstalk 1934
Amazon Elastic Block Store 1955
Amazon Elastic Container Registry 1960
Amazon Elastic Container Registry Public 1974
AWS Reprise après sinistre élastique 1981
Amazon Elastic File System 2018
Amazon Elastic Kubernetes Service 2031
AWS Elastic Load Balancing 2057
AWS Elastic Load Balancing V2 2075
Amazon Elastic MapReduce 2109
Amazon Elastic Transcoder 2129
Amazon Elastic VMware Service 2134
Amazon ElastiCache 2151
AWS Appliances et logiciels Elemental 2215
AWS Service d'activation des appliances élémentaires et des logiciels 2219
AWS Inférence élémentaire 2224
AWS Élémentaire MediaConnect 2228
AWS Élémentaire MediaConvert 2252
AWS Élémentaire MediaLive 2263
AWS Élémentaire MediaPackage 2292
AWS Élémentaire V2 MediaPackage 2299
AWS VOD élémentaire MediaPackage 2311
AWS Élémentaire MediaStore 2318
AWS Élémentaire MediaTailor 2325
AWS Dossiers de support élémentaires 2337
AWS Contenu de support élémentaire 2343
Amazon EMR on EKS (EMR Containers) 2345
Amazon EMR Serverless 2354
AWS Messagerie vocale et SMS pour l'utilisateur final V2 2361

AWS Messagerie sociale destinée aux utilisateurs finaux 2383
AWS Résolution de l'entité 2390
Amazon EventBridge 2400
Amazon EventBridge Pipes 2420
Amazon EventBridge Scheduler 2425
EventBridge Schémas Amazon 2431
AWS Service d'injection de défauts 2440
Amazon FinSpace 2451
FinSpace API Amazon 2466
AWS Firewall Manager 2469
Amazon Forecast 2482
Amazon Fraud Detector 2504
AWS Niveau gratuit 2536
Amazon FreeRTOS 2539
Amazon FSx 2545
GameLift Serveurs Amazon 2571
Amazon GameLift Streams 2601
AWS Accélérateur mondial 2608
AWS Glue 2621
AWS Glue DataBrew 2697
AWS Ground Station 2709
GroundTruth Étiquetage Amazon 2719
Amazon GuardDuty 2724
AWS Santé APIs et notifications 2745
AWS HealthImaging 2751
AWS HealthLake 2761
AWS HealthOmics 2771
Amazon Honeycode 2793
AWS Analyseur d'accès IAM 2800
AWS Centre d'identité IAM 2809
AWS Répertoire du centre d'identité IAM 2841
AWS Service OIDC du centre d'identité IAM 2853
AWS Les rôles de gestion des identités et des accès n'importe où 2857
AWS Boutique d'identités 2865
AWS Authentification du magasin d'identités 2879
AWS Synchronisation des identités 2882

AWS Service d'importation et d'exportation de disques 2887
Amazon Inspector 2890
Amazon Inspector2 2900
Canal de télémétrie Amazon Inspector2 2919
Amazon InspectorScan 2922
Amazon Interactive Video Service 2924
Amazon Interactive Video Service Chat 2945
AWS Interconnecter 2951
AWS Service de facturation 2956
AWS IoT Analytics 2964
AWS Conseiller en matière d'appareils IoT Core 2972
AWS Testeur d'appareils IoT 2978
AWS Événements liés à l'IoT 2981
AWS IoT Fleet Hub pour la gestion des appareils 2990
AWS IoT FleetWise 2995
AWS IoT Greengrass 3010
AWS IoT Greengrass V2 3034
AWS Emplois dans l'IoT DataPlane 3046
AWS Intégrations gérées par l'IoT 3049
AWS IoT SiteWise 3067
AWS IoT TwinMaker 3090
AWS IoT Wireless 3102
AWS IQ 3129
AWS Autorisations IQ 3140
Amazon Kendra 3144
Amazon Kendra Intelligent Ranking 3160
Amazon Keyspaces (for Apache Cassandra) 3165
Amazon Kinesis Analytics 3172
Amazon Kinesis Analytics V2 3177
Amazon Kinesis Data Streams 3185
Amazon Kinesis Firehose 3198
Amazon Kinesis Video Streams 3203
AWS Formation lacustre 3214
AWS Lambda 3226
AWS Launch Wizard 3250
Amazon Lex 3259

Amazon Lex V2 3270
AWS License Manager 3296
AWS License Manager (gestionnaire d'abonnements Linux) 3310
AWS Abonnements des utilisateurs de License Manager 3315
Amazon Lightsail 3323
Amazon Location 3362
Cartes Amazon Location Service 3377
Emplacements Amazon Location Service 3380
Routes Amazon Location Service 3383
Amazon Lookout for Equipment 3387
Amazon Lookout for Metrics 3400
Amazon Lookout for Vision 3409
Amazon Machine Learning 3416
Amazon Macie 3423
AWS Tests d'applications de modernisation du mainframe 3443
AWS Service de modernisation des ordinateurs centraux 3453
Amazon Managed Blockchain 3464
Amazon Managed Blockchain Query 3476
Amazon Managed Grafana 3479
Amazon Managed Service for Prometheus 3488
Amazon Managed Streaming for Apache Kafka 3507
Amazon Managed Streaming for Kafka Connect 3528
Amazon Managed Workflows for Apache Airflow 3538
AWS Marketplace 3544
AWS Marketplace Catalogue 3553
AWS Marketplace Service d'analyse du commerce 3559
AWS Marketplace Service de déploiement 3562
AWS Marketplace Découverte 3567
AWS Marketplace Service d'admissibilité 3569
AWS Marketplace Service de création d'images 3572
AWS Marketplace Portail de gestion 3575
AWS Marketplace Service de comptage 3579
AWS Marketplace Marketplace privée 3583
AWS Marketplace Intégration des systèmes d'approvisionnement 3588
AWS Marketplace Présentation de rapports 3591
AWS Marketplace Rapports sur les vendeurs 3594

AWS Marketplace Informations sur les fournisseurs 3596
AWS Serveur MCP 3605
Amazon Mechanical Turk 3608
Amazon MemoryDB 3617
Amazon Message Delivery Service 3643
Amazon Message Gateway Service 3647
AWS Extracteur de microservices pour .NET 3650
AWS Crédits du programme Migration Acceleration 3653
AWS Hub de migration 3656
AWS Migration Hub Orchestrator 3666
AWS Espaces de refactorisation du Hub de migration 3674
AWS Recommandations relatives à la stratégie du Migration Hub 3694
Amazon Mobile Analytics 3701
Amazon Monitron 3703
Amazon MQ 3714
Approbation multipartite 3724
AWS MWAA sans serveur 3733
Amazon Neptune 3739
Amazon Neptune Analytics 3746
AWS Network Firewall 3764
Network Flow Monitor 3785
AWS Directeur du réseau 3793
AWS Chat du gestionnaire de réseau 3820
Amazon Nimble Studio 3823
Loi Amazon Nova 3844
Amazon One Enterprise 3850
Amazon OpenSearch 3860
OpenSearch Ingestion d'Amazon 3864
Amazon OpenSearch sans serveur 3873
Amazon OpenSearch Service 3884
AWS OpsWorks 3913
AWS OpsWorks Gestion de configuration 3926
AWS Organisations 3931
AWS Outposts 3952
AWS Panorama 3961
AWS Service de calcul parallèle 3970

AWS Partner Central 3986
AWS Gestion centralisée des comptes pour les partenaires 4036
AWS Cryptographie des paiements 4040
AWS Paiements 4059
AWS Informations sur les Performances 4066
Amazon Personalize 4073
Amazon Pinpoint 4086
Amazon Pinpoint Email Service 4117
Amazon Pinpoint SMS and Voice Service 4133
Amazon Polly 4137
AWS Liste de prix 4141
AWS PricingPlanManager Service 4144
AWS Connecteur CA privé pour Active Directory 4147
AWS Connecteur CA privé pour SCEP 4156
AWS Autorité de certification privée 4162
AWS PrivateLink 4170
AWS Proton 4172
AWS Console de bons de commande 4203
Amazon Q 4210
Amazon Q Business 4223
Applications Amazon Q Business Q 4246
Amazon Q Developer 4263
Amazon Q in Connect 4267
Amazon QLDB 4290
Amazon QuickSight 4299
API de données Amazon RDS 4357
Authentification IAM Amazon RDS 4361
AWS Corbeille 4364
Amazon Redshift 4371
API de données Amazon Redshift 4419
Amazon Redshift sans serveur 4426
Amazon Rekognition 4449
AWS Republier en privé 4466
AWS Centre de résilience 4472
AWS Resource Access Manager (RAM) 4490
AWS Explorateur de ressources 4512

API de balisage des groupes de ressources Amazon 4522
AWS Resource Groups 4526
Portail de la RHEL Knowledgebase Amazon. 4534
AWS RoboMaker 4536
Amazon Route 53 4551
Amazon Route 53 Domaines 4569
Profils Amazon Route 53 4577
Amazon Route 53 Recovery Cluster 4586
Amazon Route 53 Recovery Controls 4590
Amazon Route 53 Recovery Readiness 4598
Amazon Route 53 Resolver 4607
AWS Résolveur global Route53 4632
AWS Tissu RTB 4643
Amazon S3 Express 4653
Amazon S3 Glacier 4691
Amazon S3 Object Lambda 4699
Amazon S3 on Outposts 4728
Tables Amazon S3 4797
Amazon S3 Vectors 4814
Assistant en science SageMaker des données Amazon 4828
Fonctionnalités SageMaker géospatiales d'Amazon 4830
Amazon SageMaker Unified Studio MCP 4839
Amazon SageMaker avec MLflow 4842
AWS Savings Plans 4852
AWS Secrets Manager 4857
AWS Agent de sécurité 4896
AWS Security Hub 4911
AWS Réponse aux incidents de sécurité 4939
Amazon Security Lake 4947
AWS Service de migration de serveurs 4981
AWS Serverless Application Repository 4988
AWS Service - Base de données Oracle@AWS 4994
AWS Service Catalog 5011
AWS service fournissant des réseaux privés gérés 5040
Service Quotas 5048
Amazon SES 5059

AWS Shield 5079
AWS Directeur de la sécurité du réseau Shield 5092
AWS Signataire 5095
AWS Se connecter 5102
Amazon Simple Email Service - Gestionnaire de messagerie 5107
Amazon Simple Email Service v2 5125
Amazon Simple Workflow Service 5165
Amazon SimpleDB 5183
AWS SimSpace Tisserand 5188
AWS Gestion des appareils Snow 5193
AWS Snowball 5198
Amazon SNS 5205
AWS Banc de travail SQL 5216
Amazon SQS 5236
AWS Step Functions 5242
AWS Storage Gateway 5254
AWS Chaîne d'approvisionnement 5280
AWS Support 5290
AWS Support App dans Slack 5299
AWS Support Console 5303
AWS Support Plans 5307
AWS Durabilité 5310
AWS Systems Manager pour SAP 5313
AWS Systems Manager GUI Connect 5322
AWS Systems Manager Gestionnaire des incidents 5326
AWS Contacts du responsable des incidents de Systems Manager 5335
AWS Configuration rapide de Systems Manager 5344
Tag Editor 5350
AWS Paramètres fiscaux 5352
AWS Générateur de réseaux de télécommunications 5358
Amazon Textract 5369
Amazon Timestream 5376
Amazon Timestream InfluxDB 5388
AWS Tiros 5396
Amazon Transcribe 5399
AWS Transfer Family 5417

AWS Transformation 5435
AWS Transformez sur mesure 5441
Amazon Translate 5449
AWS Trusted Advisor 5456
AWS Personnalisation de l'expérience utilisateur 5468
AWS Notifications aux utilisateurs 5471
AWS Contacts pour les notifications des utilisateurs 5482
AWS Abonnements d'utilisateurs 5486
AWS Accès vérifié 5490
Amazon Verified Permissions 5492
Amazon VPC Lattice 5500
Services Amazon VPC Lattice 5540
AWS WAF 5546
AWS WAF régional 5561
AWS WAF V2 5577
AWS Outil Well-Architected 5601
AWS Osier 5619
Amazon WorkDocs 5628
Amazon WorkLink 5640
Amazon WorkMail 5649
Flux de WorkMail messages Amazon 5673
Amazon WorkSpaces 5676
Gestionnaire WorkSpaces d'applications Amazon 5699
AWS WorkSpaces Instances gérées 5701
Navigateur Amazon WorkSpaces Secure 5706
Amazon WorkSpaces Thin Client 5727
AWS X-Ray 5736
Ressources connexes 5748
Accès programmatique aux informations de référence des services 5749
Glossaire 5755
Définitions de champs supplémentaires 5755
..... 5758

Référence

La référence d'autorisation de service fournit une liste des actions, des ressources et des clés de condition prises en charge par chaque AWS service. Vous pouvez spécifier des actions, des ressources et des clés de condition dans les politiques Gestion des identités et des accès AWS (IAM) pour gérer l'accès aux AWS ressources.

Table des matières

- Actions, ressources et clés de condition pour les AWS services
- Ressources connexes

Actions, ressources et clés de condition pour les AWS services

Chaque AWS service peut définir des actions, des ressources et des clés de contexte de condition à utiliser dans les politiques IAM. Cette rubrique décrit la façon dont les éléments fournis pour chaque service sont documentés.

Chaque rubrique se compose de tableaux répertoriant des actions, ressources et clés de condition disponibles.

Tableau Actions

Le tableau Actions répertorie toutes les actions que vous pouvez utiliser dans l'élément `Action` d'une déclaration de politique IAM. Certaines opérations d'API définies par un service ne peuvent pas être utilisées en guise d'action dans une politique IAM. Certains services incluent des actions avec autorisations uniquement qui ne correspondent pas directement à une opération d'API. Ces actions sont indiquées avec [autorisation uniquement]. Utilisez cette liste pour déterminer quelles actions utiliser dans une politique IAM. Pour de plus amples informations sur les éléments `Action`, `Resource` ou `Condition`, veuillez consulter le document Référence des éléments de politique JSON IAM. Les colonnes Actions et Description du tableau sont auto-descriptives.

- La colonne Access Level (Niveau d'accès) spécifie la façon dont l'action est classée (Liste, Lecture, Écriture, Gestion des autorisations ou Balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour de plus amples informations sur les niveaux d'accès, veuillez consultez Présentation des récapitulatifs de niveau d'accès au sein des récapitulatifs de politiques.

- La colonne Resource Types (Types de ressources) indique si l'action prend en charge les autorisations au niveau des ressources. Si la colonne est vide, l'action ne prend pas en charge les autorisations au niveau des ressources et vous devez spécifier toutes les ressources (« * ») dans votre politique. Si la colonne inclut un type de ressource, vous pouvez spécifier l'ARN de la ressource dans l'élément `Resource` de votre politique. Pour de plus amples informations sur cette ressource, veuillez consulter cette ligne dans le tableau Resource types (Types de ressources). Toutes les actions et ressources incluses dans une déclaration doivent être mutuellement compatibles. Si vous spécifiez une ressource qui n'est pas valide pour l'action, toute demande d'utilisation de cette action échoue et l'élément `Effect` de la déclaration ne s'applique pas.

  Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous indiquez un ARN d'autorisation au niveau des ressources dans une déclaration à l'aide de cette action, il doit être de ce type. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.
- La colonne Condition keys (Clés de condition) inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Les clés de condition peuvent être prises en charge avec une action, ou avec une action et une ressource spécifique. Veillez à ce que la clé se trouve sur la même ligne qu'un type de ressource spécifique. Cette table n'inclut pas les clés de condition globales qui sont disponibles pour toute action ou dans des circonstances indépendantes. Pour de plus amples informations sur les clés de condition globales, veuillez consulter Clés de contexte de condition globales AWS.
- La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

  Les actions dépendantes ne sont pas requises dans tous les scénarios. Reportez-vous à la documentation de chaque service pour plus d'informations sur l'octroi d'autorisations granulaires aux utilisateurs.

Tableau Types de ressources

Le tableau Resource Types (Types de ressources) répertorie tous les types de ressources que vous pouvez spécifier en tant qu'ARN dans l'élément de politique `Resource`. Tous les types de ressources ne peuvent pas être spécifiés avec chaque action. Certains types de ressources fonctionnent avec

seulement certaines actions. Si vous spécifiez un type de ressource dans une déclaration avec une action qui ne prend pas en charge ce type de ressource, la déclaration n'autorise pas l'accès. Pour de plus amples informations sur l'élément `Resource`, veuillez consulter Éléments de politique JSON IAM : ressource.

- La colonne ARN spécifie le format Amazon Resource Name (ARN) à utiliser pour référencer des ressources de ce type. Les parties précédées d'un symbole $ doivent être remplacées par les valeurs réelles de votre scénario. Par exemple, si `$user-name` s'affiche dans un ARN, vous devez remplacer cette chaîne par le nom de l'utilisateur ou une variable de stratégie contenant le nom d'un utilisateur. Pour plus d'informations sur ARNs, consultez la section IAM ARNs.
- La colonne Condition keys (Clés de condition) spécifie les clés de contexte de condition que vous pouvez inclure dans une déclaration de politique IAM uniquement lorsque cette action et cette ressource sont incluses dans la déclaration.

Tableau Clés de condition

Le tableau Condition keys (Clés de condition) répertorie toutes les clés de contexte de condition que vous pouvez utiliser dans l'élément `Condition` d'une déclaration de politique IAM. Certaines clés ne peuvent pas être spécifiées avec chaque action ou ressource. Certaines clés fonctionnent uniquement avec certains types d'actions et de ressources. Pour de plus amples informations sur l'élément `Condition`, veuillez consulter Éléments de politique JSON IAM : condition.

- La colonne Type spécifie le type de données de la clé de condition. Ce type de données détermine les opérateurs de condition que vous pouvez utiliser pour comparer les valeurs de la demande avec les valeurs de la déclaration de politique. Vous devez utiliser un opérateur correspondant au type de données. Dans le cas contraire, la correspondance échoue toujours et la déclaration de politique ne s'applique jamais.

  Si la colonne Type spécifie une « Liste de... » l'un des types simples, vous pouvez alors utiliser plusieurs clés et valeurs dans vos stratégies. Pour cela, utilisez des préfixes de définition de condition avec vos opérateurs. Utilisez le préfixe `ForAllValues` pour spécifier que toutes les valeurs de la demande doivent correspondre à une valeur de la déclaration de politique. Utilisez le préfixe `ForAnyValue` pour spécifier qu'au moins une valeur de la demande correspond à l'une des valeurs de la déclaration de politique.

Rubriques

- Actions, ressources et clés de condition pour la gestion des AWS comptes
- Actions, ressources et clés de condition pour les recommandations AWS d'action
- Actions, ressources et clés de condition pour AWS Activate
- Actions, ressources et clés de condition pour Amazon AI Operations
- Actions, ressources et clés de condition pour Alexa for Business
- Actions, ressources et clés de condition pour AmazonMediaImport
- Actions, ressources et clés de condition pour AWS Amplify
- Actions, ressources et clés de condition pour AWS Amplify Admin
- Actions, ressources et clés de condition pour AWS Amplify UI Builder
- Actions, ressources et clés de condition pour les clusters Apache Kafka APIs pour Amazon MSK
- Actions, ressources et clés de condition pour Amazon API Gateway
- Actions, ressources et clés de condition pour AWS App Mesh
- Actions, ressources et clés de condition pour AWS App Mesh Preview
- Actions, ressources et clés de condition pour AWS App Runner
- Actions, ressources et clés de condition pour AWS App Studio
- Actions, ressources et clés de condition pour AWS App2Container
- Actions, ressources et clés de condition pour AWS AppConfig
- Actions, ressources et clés de condition pour AWS AppFabric
- Actions, ressources et clés de condition pour Amazon AppFlow
- Actions, ressources et clés de condition pour Amazon AppIntegrations
- Actions, ressources et clés de condition pour AWS Application Auto Scaling
- Actions, ressources et clés de condition pour Application Discovery Arsenal
- Actions, ressources et clés de condition pour AWS Application Discovery Service
- Actions, ressources et clés de condition pour le service de migration AWS d'applications
- Actions, ressources et clés de condition pour Amazon Application Recovery Controller - Zonal Shift
- Actions, ressources et clés de condition pour le service de transformation des AWS applications
- Actions, ressources et clés de condition pour Amazon AppStream 2.0
- Actions, ressources et clés de condition pour AWS AppSync
- Actions, ressources et clés de condition pour le changement de région Amazon ARC
- Actions, ressources et clés de condition pour AWS Artifact

- Actions, ressources et clés de condition pour Amazon Athena
- Actions, ressources et clés de condition pour AWS Audit Manager
- Actions, ressources et clés de condition pour Amazon Aurora DSQL
- Actions, ressources et clés de condition pour AWS Auto Scaling
- Actions, ressources et clés de condition pour l'échange de données AWS B2B
- Actions, ressources et clés de condition pour AWS Backup
- Actions, ressources et clés de condition pour AWS Backup Gateway
- Actions, ressources et clés de condition pour AWS Backup Search
- Actions, ressources et clés de condition pour le stockage des AWS sauvegardes
- Actions, ressources et clés de condition pour AWS Batch
- Actions, ressources et clés de condition pour Amazon Bedrock
- Actions, ressources et clés de condition pour Amazon Bedrock Agentcore
- Actions, ressources et clés de condition pour Amazon Bedrock Powered by AWS Mantle
- Actions, ressources et clés de condition pour AWS Billing
- Actions, ressources et clés de condition pour les tableaux AWS Billing de bord de gestion des coûts
- Actions, ressources et clés de condition pour les exportations AWS Billing de données de gestion des coûts
- Actions, ressources et clés de condition pour le calculateur de prix AWS Billing And Cost Management
- Actions, ressources et clés de condition pour les actions recommandées par AWS Billing And Cost Management
- Actions, ressources et clés de condition pour AWS Billing Conductor
- Actions, ressources et clés de condition pour AWS Billing la console
- Actions, ressources et clés de condition pour Amazon Braket
- Actions, ressources et clés de condition pour AWS Budget Service
- Actions, ressources et clés de condition pour AWS BugBust
- Actions, ressources et clés de condition pour AWS Certificate Manager
- Actions, ressources et clés de condition pour AWS Chatbot
- Actions, ressources et clés de condition pour Amazon Chime
- Actions, ressources et clés de condition pour Claude Platform sur AWS

- Actions, ressources et clés de condition pour les salles AWS blanches
- Actions, ressources et clés de condition pour AWS Clean Rooms ML
- Actions, ressources et clés de condition pour l'API AWS Cloud de contrôle
- Actions, ressources et clés de condition pour Amazon Cloud Directory
- Actions, ressources et clés de condition pour AWS Cloud la carte
- Actions, ressources et clés de condition pour AWS Cloud9
- Actions, ressources et clés de condition pour AWS CloudFormation
- Actions, ressources et clés de condition pour Amazon CloudFront
- Actions, ressources et clés de condition pour Amazon CloudFront KeyValueStore
- Actions, ressources et clés de condition pour AWS CloudHSM
- Actions, ressources et clés de condition pour Amazon CloudSearch
- Actions, ressources et clés de condition pour AWS CloudShell
- Actions, ressources et clés de condition pour AWS CloudTrail
- Actions, ressources et clés de condition pour les AWS CloudTrail données
- Actions, ressources et clés de condition pour Amazon CloudWatch
- Actions, ressources et clés de condition pour Amazon CloudWatch Application Insights
- Actions, ressources et clés de condition pour Amazon CloudWatch Application Signals
- Actions, ressources et clés de condition pour Amazon CloudWatch Evidently
- Actions, ressources et clés de condition pour Amazon CloudWatch Internet Monitor
- Actions, ressources et clés de condition pour Amazon CloudWatch Logs
- Actions, ressources et clés de condition pour Amazon CloudWatch Network Synthetic Monitor
- Actions, ressources et clés de condition pour Amazon CloudWatch Observability Access Manager
- Actions, ressources et clés de condition pour Amazon CloudWatch Observability Admin Service
- Actions, ressources et clés de condition pour AWS CloudWatch RUM
- Actions, ressources et clés de condition pour Amazon CloudWatch Synthetics
- Actions, ressources et clés de condition pour AWS CodeArtifact
- Actions, ressources et clés de condition pour Amazon CodeCatalyst
- Actions, ressources et clés de condition pour AWS CodeCommit
- Actions, ressources et clés de condition pour AWS CodeConnections
- Actions, ressources et clés de condition pour AWS CodeDeploy

- Actions, ressources et clés de condition pour un service de commandes hôte AWS CodeDeploy sécurisé
- Actions, ressources et clés de condition pour Amazon CodeGuru
- Actions, ressources et clés de condition pour Amazon CodeGuru Profiler
- Actions, ressources et clés de condition pour Amazon CodeGuru Reviewer
- Actions, ressources et clés de condition pour Amazon CodeGuru Security
- Actions, ressources et clés de condition pour AWS CodePipeline
- Actions, ressources et clés de condition pour AWS CodeStar
- Actions, ressources et clés de condition pour les AWS CodeStar connexions
- Actions, ressources et clés de condition pour les AWS CodeStar notifications
- Actions, ressources et clés de condition pour Amazon CodeWhisperer
- Actions, ressources et clés de condition pour Amazon Cognito Identity
- Actions, ressources et clés de condition pour Amazon Cognito Sync
- Actions, ressources et clés de condition pour Amazon Cognito User Pools
- Actions, ressources et clés de condition pour Amazon Comprehend
- Actions, ressources et clés de condition pour Amazon Comprehend Medical
- Actions, ressources et clés de condition pour AWS Compute Optimizer
- Actions, ressources et clés de condition pour AWS Compute Optimizer Automation
- Actions, ressources et clés de condition pour AWS Config
- Actions, ressources et clés de condition pour Amazon Connect Cases
- Actions, ressources et clés de condition pour Amazon Connect Customer Profiles
- Actions, ressources et clés de condition pour Amazon Connect Health
- Actions, ressources et clés de condition pour les campagnes sortantes Amazon Connect
- Actions, ressources et clés de condition pour Amazon Connect Voice ID
- Actions, ressources et clés de condition pour AWS Connector Service
- Actions, ressources et clés de condition pour l'application AWS Management Console mobile
- Actions, ressources et clés de condition pour la facturation AWS consolidée
- Actions, ressources et clés de condition pour AWS Control Catalog
- Actions, ressources et clés de condition pour AWS Control Tower
- Actions, ressources et clés de condition pour le rapport sur les AWS coûts et l'utilisation

- Actions, ressources et clés de condition pour le service AWS Cost Explorer
- Actions, ressources et clés de condition pour le hub d'optimisation des AWS coûts
- Actions, ressources et clés de condition pour le service de vérification AWS client
- Actions, ressources et clés de condition pour AWS Data Exchange
- Actions, ressources et clés de condition pour Amazon Data Lifecycle Manager
- Actions, ressources et clés de condition pour AWS Data Pipeline
- Actions, ressources et clés de condition pour le service AWS de migration de base de données
- Actions, ressources et clés de condition pour Database Query Metadata Service
- Actions, ressources et clés de condition pour AWS DataSync
- Actions, ressources et clés de condition pour Amazon DataZone
- Actions, ressources et clés de condition pour AWS Deadline Cloud
- Actions, ressources et clés de condition pour Amazon Detective
- Actions, ressources et clés de condition pour AWS Device Farm
- Actions, ressources et clés de condition pour le service AWS DevOps d'agent
- Actions, ressources et clés de condition pour Amazon DevOps Guru
- Actions, ressources et clés de condition pour les outils AWS de diagnostic
- Actions, ressources et clés de condition pour AWS Direct Connect
- Actions, ressources et clés de condition pour AWS Directory Service
- Actions, ressources et clés de condition pour les données du service de AWS répertoire
- Actions, ressources et clés de condition pour les clusters Amazon DocumentDB Elastic
- Actions, ressources et clés de condition pour Amazon DynamoDB
- Actions, ressources et clés de condition pour Amazon DynamoDB Accelerator (DAX)
- Actions, ressources et clés de condition pour Amazon EC2 Auto Scaling
- Actions, ressources et clés de condition pour Amazon EC2 Image Builder
- Actions, ressources et clés de condition pour Amazon EC2 Instance Connect
- Actions, ressources et clés de condition pour le service Amazon ECS MCP
- Actions, ressources et clés de condition pour Amazon EKS Auth
- Actions, ressources et clés de condition pour le serveur Amazon EKS MCP
- Actions, ressources et clés de condition pour AWS Elastic Beanstalk
- Actions, ressources et clés de condition pour Amazon Elastic Block Store

- Actions, ressources et clés de condition pour Amazon Elastic Container Registry
- Actions, ressources et clés de condition pour Amazon Elastic Container Registry Public
- Actions, ressources et clés de condition pour AWS Elastic Disaster Recovery
- Actions, ressources et clés de condition pour Amazon Elastic File System
- Actions, ressources et clés de condition pour Amazon Elastic Kubernetes Service
- Actions, ressources et clés de condition pour AWS Elastic Load Balancing
- Actions, ressources et clés de condition pour AWS Elastic Load Balancing V2
- Actions, ressources et clés de condition pour Amazon Elastic MapReduce
- Actions, ressources et clés de condition pour Amazon Elastic Transcoder
- Actions, ressources et clés de condition pour Amazon Elastic VMware Service
- Actions, ressources et clés de condition pour Amazon ElastiCache
- Actions, ressources et clés de condition pour les appareils et AWS logiciels Elemental
- Actions, ressources et clés de condition pour les appliances AWS élémentaires et le service d'activation logicielle
- Actions, ressources et clés de condition pour l' AWS inférence élémentaire
- Actions, ressources et clés de condition pour AWS Elemental MediaConnect
- Actions, ressources et clés de condition pour AWS Elemental MediaConvert
- Actions, ressources et clés de condition pour AWS Elemental MediaLive
- Actions, ressources et clés de condition pour AWS Elemental MediaPackage
- Actions, ressources et clés de condition pour AWS Elemental V2 MediaPackage
- Actions, ressources et clés de condition pour AWS Elemental VOD MediaPackage
- Actions, ressources et clés de condition pour AWS Elemental MediaStore
- Actions, ressources et clés de condition pour AWS Elemental MediaTailor
- Actions, ressources et clés de condition pour les cas de support AWS élémentaire
- Actions, ressources et clés de condition pour le contenu de support AWS élémentaire
- Actions, ressources et clés de condition pour Amazon EMR on EKS (EMR Containers)
- Actions, ressources et clés de condition pour Amazon EMR Serverless
- Actions, ressources et clés de condition pour AWS la messagerie SMS et voix de l'utilisateur final V2
- Actions, ressources et clés de condition pour AWS la messagerie sociale destinée aux utilisateurs finaux

- Actions, ressources et clés de condition pour la résolution AWS d'entités
- Actions, ressources et clés de condition pour Amazon EventBridge
- Actions, ressources et clés de condition pour Amazon EventBridge Pipes
- Actions, ressources et clés de condition pour Amazon EventBridge Scheduler
- Actions, ressources et clés de condition pour Amazon EventBridge Schemas
- Actions, ressources et clés de condition pour le service d'injection de AWS défauts
- Actions, ressources et clés de condition pour Amazon FinSpace
- Actions, ressources et clés de condition pour l' FinSpace API Amazon
- Actions, ressources et clés de condition pour AWS Firewall Manager
- Actions, ressources et clés de condition pour Amazon Forecast
- Actions, ressources et clés de condition pour Amazon Fraud Detector
- Actions, ressources et clés de condition pour le niveau AWS gratuit
- Actions, ressources et clés de condition pour Amazon FreeRTOS
- Actions, ressources et clés de condition pour Amazon FSx
- Actions, ressources et clés de condition pour les GameLift serveurs Amazon
- Actions, ressources et clés de condition pour Amazon GameLift Streams
- Actions, ressources et clés de condition pour AWS Global Accelerator
- Actions, ressources et clés de condition pour AWS Glue
- Actions, ressources et clés de condition pour AWS Glue DataBrew
- Actions, ressources et clés de condition pour AWS Ground Station
- Actions, ressources et clés de condition pour Amazon GroundTruth Labeling
- Actions, ressources et clés de condition pour Amazon GuardDuty
- Actions, ressources et clés de condition pour AWS Health APIs and Notifications
- Actions, ressources et clés de condition pour AWS HealthImaging
- Actions, ressources et clés de condition pour AWS HealthLake
- Actions, ressources et clés de condition pour AWS HealthOmics
- Actions, ressources et clés de condition pour Amazon Honeycode
- Actions, ressources et clés de condition pour AWS IAM Access Analyzer
- Actions, ressources et clés de condition pour AWS IAM Identity Center
- Actions, ressources et clés de condition pour le répertoire AWS IAM Identity Center

- Actions, ressources et clés de condition pour le service AWS IAM Identity Center OIDC
- Actions, ressources et clés de condition pour AWS Identity and Access Management Roles Anywhere
- Actions, ressources et clés de condition pour AWS Identity Store
- Actions, ressources et clés de condition pour AWS Identity Store Auth
- Actions, ressources et clés de condition pour AWS Identity Sync
- Actions, ressources et clés de condition pour le service AWS Import Export Disk
- Actions, ressources et clés de condition pour Amazon Inspector
- Actions, ressources et clés de condition pour Amazon Inspector2
- Actions, ressources et clés de condition pour le canal de télémétrie Amazon Inspector2
- Actions, ressources et clés de condition pour Amazon InspectorScan
- Actions, ressources et clés de condition pour Amazon Interactive Video Service
- Actions, ressources et clés de condition pour Amazon Interactive Video Service Chat
- Actions, ressources et clés de condition pour l' AWS interconnexion
- Actions, ressources et clés de condition pour le service de AWS facturation
- Actions, ressources et clés de condition pour AWS IoT Analytics
- Actions, ressources et clés de condition pour AWS IoT Core Device Advisor
- Actions, ressources et clés de condition pour le testeur d'appareils AWS IoT
- Actions, ressources et clés de condition pour AWS IoT Events
- Actions, ressources et clés de condition pour AWS IoT Fleet Hub pour la gestion des appareils
- Actions, ressources et clés de condition pour AWS l'IoT FleetWise
- Actions, ressources et clés de condition pour AWS IoT Greengrass
- Actions, ressources et clés de condition pour AWS IoT Greengrass V2
- Actions, ressources et clés de condition pour les emplois liés à AWS l'IoT DataPlane
- Actions, ressources et clés de condition pour les intégrations gérées par AWS l'IoT
- Actions, ressources et clés de condition pour AWS l'IoT SiteWise
- Actions, ressources et clés de condition pour AWS l'IoT TwinMaker
- Actions, ressources et clés de condition pour AWS IoT Wireless
- Actions, ressources et clés de condition pour AWS IQ
- Actions, ressources et clés de condition pour AWS IQ Permissions

- Actions, ressources et clés de condition pour Amazon Kendra
- Actions, ressources et clés de condition pour Amazon Kendra Intelligent Ranking
- Actions, ressources et clés de condition pour Amazon Keyspaces (for Apache Cassandra)
- Actions, ressources et clés de condition pour Amazon Kinesis Analytics
- Actions, ressources et clés de condition pour Amazon Kinesis Analytics V2
- Actions, ressources et clés de condition pour Amazon Kinesis Data Streams
- Actions, ressources et clés de condition pour Amazon Kinesis Firehose
- Actions, ressources et clés de condition pour Amazon Kinesis Video Streams
- Actions, ressources et clés de condition pour AWS Lake Formation
- Actions, ressources et clés de condition pour AWS Lambda
- Actions, ressources et clés de condition pour AWS Launch Wizard
- Actions, ressources et clés de condition pour Amazon Lex
- Actions, ressources et clés de condition pour Amazon Lex V2
- Actions, ressources et clés de condition pour AWS License Manager
- Actions, ressources et clés de condition pour AWS License Manager Linux Subscriptions Manager
- Actions, ressources et clés de condition pour les abonnements utilisateurs AWS de License Manager
- Actions, ressources et clés de condition pour Amazon Lightsail
- Actions, ressources et clés de condition pour Amazon Location
- Actions, ressources et clés de condition pour les cartes Amazon Location Service
- Actions, ressources et clés de condition pour Amazon Location Service Places
- Actions, ressources et clés de condition pour Amazon Location Service Routes
- Actions, ressources et clés de condition pour Amazon Lookout for Equipment
- Actions, ressources et clés de condition pour Amazon Lookout for Metrics
- Actions, ressources et clés de condition pour Amazon Lookout for Vision
- Actions, ressources et clés de condition pour Amazon Machine Learning
- Actions, ressources et clés de condition pour Amazon Macie
- Actions, ressources et clés de condition pour les tests d'applications de modernisation AWS du mainframe
- Actions, ressources et clés de condition pour le service de modernisation AWS du mainframe
- Actions, ressources et clés de condition pour Amazon Managed Blockchain

- Actions, ressources et clés de condition pour Amazon Managed Blockchain Query
- Actions, ressources et clés de condition pour Amazon Managed Grafana
- Actions, ressources et clés de condition pour Amazon Managed Service for Prometheus
- Actions, ressources et clés de condition pour Amazon Managed Streaming for Apache Kafka
- Actions, ressources et clés de condition pour Amazon Managed Streaming for Kafka Connect
- Actions, ressources et clés de condition pour Amazon Managed Workflows for Apache Airflow
- Actions, ressources et clés de condition pour AWS Marketplace
- Actions, ressources et clés de condition pour le AWS Marketplace catalogue
- Actions, ressources et clés de condition pour AWS Marketplace le service Commerce Analytics
- Actions, ressources et clés de condition pour AWS Marketplace le service de déploiement
- Actions, ressources et clés de condition pour AWS Marketplace Discovery
- Actions, ressources et clés de condition pour AWS Marketplace Entitlement Service
- Actions, ressources et clés de condition pour AWS Marketplace Image Building Service
- Actions, ressources et clés de condition pour le portail AWS Marketplace de gestion
- Actions, ressources et clés de condition pour le service AWS Marketplace de mesure
- Actions, ressources et clés de condition pour AWS Marketplace Private Marketplace
- Actions, ressources et clés de condition pour l'intégration AWS Marketplace des systèmes d'approvisionnement
- Actions, ressources et clés de condition pour les AWS Marketplace rapports
- Actions, ressources et clés de condition pour les rapports sur les AWS Marketplace vendeurs
- Actions, ressources et clés de condition pour AWS Marketplace Vendor Insights
- Actions, ressources et clés de condition pour le serveur AWS MCP
- Actions, ressources et clés de condition pour Amazon Mechanical Turk
- Actions, ressources et clés de condition pour Amazon MemoryDB
- Actions, ressources et clés de condition pour Amazon Message Delivery Service
- Actions, ressources et clés de condition pour Amazon Message Gateway Service
- Actions, ressources et clés de condition pour AWS Microservice Extractor pour .NET
- Actions, ressources et clés de condition pour les crédits du programme AWS Migration Acceleration
- Actions, ressources et clés de condition pour AWS Migration Hub
- Actions, ressources et clés de condition pour AWS Migration Hub Orchestrator

- Actions, ressources et clés de condition pour AWS Migration Hub Refactor Spaces
- Actions, ressources et clés de condition pour les recommandations stratégiques du AWS Migration Hub
- Actions, ressources et clés de condition pour Amazon Mobile Analytics
- Actions, ressources et clés de condition pour Amazon Monitron
- Actions, ressources et clés de condition pour Amazon MQ
- Actions, ressources et clés de condition pour une approbation multipartite
- Actions, ressources et clés de condition pour AWS MWAA Serverless
- Actions, ressources et clés de condition pour Amazon Neptune
- Actions, ressources et clés de condition pour Amazon Neptune Analytics
- Actions, ressources et clés de condition pour AWS Network Firewall
- Actions, ressources et clés de condition pour Network Flow Monitor
- Actions, ressources et clés de condition pour AWS Network Manager
- Actions, ressources et clés de condition pour AWS Network Manager Chat
- Actions, ressources et clés de condition pour Amazon Nimble Studio
- Actions, ressources et clés de condition pour Amazon Nova Act
- Actions, ressources et clés de condition pour Amazon One Enterprise
- Actions, ressources et clés de condition pour Amazon OpenSearch
- Actions, ressources et clés de condition pour Amazon OpenSearch Ingestion
- Actions, ressources et clés de condition pour Amazon OpenSearch Serverless
- Actions, ressources et clés de condition pour Amazon OpenSearch Service
- Actions, ressources et clés de condition pour AWS OpsWorks
- Actions, ressources et clés de condition pour la gestion AWS OpsWorks de la configuration
- Actions, ressources et clés de condition pour les AWS Organizations
- Actions, ressources et clés de condition pour les AWS Outposts
- Actions, ressources et clés de condition pour AWS Panorama
- Actions, ressources et clés de condition pour le service de calcul AWS parallèle
- Actions, ressources et clés de condition pour AWS Partner Central
- Actions, ressources et clés de condition pour la gestion centrale des comptes des AWS partenaires
- Actions, ressources et clés de condition pour la cryptographie des AWS paiements
- Actions, ressources et clés de condition pour les AWS paiements

- Actions, ressources et clés de condition pour AWS Performance Insights
- Actions, ressources et clés de condition pour Amazon Personalize
- Actions, ressources et clés de condition pour Amazon Pinpoint
- Actions, ressources et clés de condition pour Amazon Pinpoint Email Service
- Actions, ressources et clés de condition pour Amazon Pinpoint SMS and Voice Service
- Actions, ressources et clés de condition pour Amazon Polly
- Actions, ressources et clés de condition pour la liste de AWS prix
- Actions, ressources et clés de condition pour le AWS PricingPlanManager service
- Actions, ressources et clés de condition pour AWS Private CA Connector for Active Directory
- Actions, ressources et clés de condition pour AWS Private CA Connector for SCEP
- Actions, ressources et clés de condition pour l'autorité de certification AWS privée
- Actions, ressources et clés de condition pour AWS PrivateLink
- Actions, ressources et clés de condition pour AWS Proton
- Actions, ressources et clés de condition pour la console des bons de AWS commande
- Actions, ressources et clés de condition pour Amazon Q
- Actions, ressources et clés de condition pour Amazon Q Business
- Actions, ressources et clés de condition pour les applications Amazon Q Business Q
- Actions, ressources et clés de condition pour Amazon Q Developer
- Actions, ressources et clés de condition pour Amazon Q in Connect
- Actions, ressources et clés de condition pour Amazon QLDB
- Actions, ressources et clés de condition pour Amazon QuickSight
- Actions, ressources et clés de condition pour l'API de données Amazon RDS
- Actions, ressources et clés de condition pour l'authentification IAM Amazon RDS
- Actions, ressources et clés de condition pour la AWS corbeille
- Actions, ressources et clés de condition pour Amazon Redshift
- Actions, ressources et clés de condition pour l'API de données Amazon Redshift
- Actions, ressources et clés de condition pour Amazon Redshift sans serveur
- Actions, ressources et clés de condition pour Amazon Rekognition
- Actions, ressources et clés de condition pour AWS RePost Private
- Actions, ressources et clés de condition pour AWS Resilience Hub

- Actions, ressources et clés de condition pour AWS Resource Access Manager (RAM)
- Actions, ressources et clés de condition pour AWS Resource Explorer
- Actions, ressources et clés de condition pour l'API de balisage des groupes de ressources Amazon
- Actions, ressources et clés de condition pour AWS Resource Groups
- Actions, ressources et clés de condition pour le portail de la RHEL Knowledgebase Amazon.
- Actions, ressources et clés de condition pour AWS RoboMaker
- Actions, ressources et clés de condition pour Amazon Route 53
- Actions, ressources et clés de condition pour Amazon Route 53 Domains
- Actions, ressources et clés de condition pour les profils Amazon Route 53
- Actions, ressources et clés de condition pour Amazon Route 53 Recovery Cluster
- Actions, ressources et clés de condition pour Amazon Route 53 Recovery Controls
- Actions, ressources et clés de condition pour Amazon Route 53 Recovery Readiness
- Actions, ressources et clés de condition pour Amazon Route 53 Resolver
- Actions, ressources et clés de condition pour AWS Route53 Global Resolver
- Actions, ressources et clés de condition pour AWS RTB Fabric
- Actions, ressources et clés de condition pour Amazon S3 Express
- Actions, ressources et clés de condition pour Amazon S3 Glacier
- Actions, ressources et clés de condition pour Amazon S3 Object Lambda
- Actions, ressources et clés de condition pour Amazon S3 on Outposts
- Actions, ressources et clés de condition pour les tables Amazon S3
- Actions, ressources et clés de condition pour les vecteurs Amazon S3
- Actions, ressources et clés de condition pour Amazon SageMaker Data Science Assistant
- Actions, ressources et clés de condition pour les fonctionnalités SageMaker géospatiales d'Amazon
- Actions, ressources et clés de condition pour Amazon SageMaker Unified Studio MCP
- Actions, ressources et clés de condition pour Amazon SageMaker avec MLflow
- Actions, ressources et clés de condition pour AWS Savings Plans
- Actions, ressources et clés de condition pour AWS Secrets Manager
- Actions, ressources et clés de condition pour AWS Security Agent
- Actions, ressources et clés de condition pour AWS Security Hub
- Actions, ressources et clés de condition pour la réponse aux incidents AWS de sécurité

- Actions, ressources et clés de condition pour Amazon Security Lake
- Actions, ressources et clés de condition pour le service de migration de AWS serveurs
- Actions, ressources et clés de condition pour AWS Serverless Application Repository
- Actions, ressources et clés de condition pour le AWS service - Oracle Database@AWS
- Actions, ressources et clés de condition pour AWS Service Catalog
- Actions, ressources et clés de condition pour les réseaux privés gérés fournissant des AWS services
- Actions, ressources et clés de condition pour Service Quotas
- Actions, ressources et clés de condition pour Amazon SES
- Actions, ressources et clés de condition pour AWS Shield
- Actions, ressources et clés de condition pour le directeur de la sécurité du réseau AWS Shield
- Actions, ressources et clés de condition pour le AWS signataire
- Actions, ressources et clés de condition pour la AWS connexion
- Actions, ressources et clés de condition pour Amazon Simple Email Service - Mail Manager
- Actions, ressources et clés de condition pour Amazon Simple Email Service v2
- Actions, ressources et clés de condition pour Amazon Simple Workflow Service
- Actions, ressources et clés de condition pour Amazon SimpleDB
- Actions, ressources et clés de condition pour AWS SimSpace Weaver
- Actions, ressources et clés de condition pour la gestion des appareils AWS Snow
- Actions, ressources et clés de condition pour AWS Snowball
- Actions, ressources et clés de condition pour Amazon SNS
- Actions, ressources et clés de condition pour AWS SQL Workbench
- Actions, ressources et clés de condition pour Amazon SQS
- Actions, ressources et clés de condition pour AWS Step Functions
- Actions, ressources et clés de condition pour AWS Storage Gateway
- Actions, ressources et clés de condition pour la chaîne AWS d'approvisionnement
- Actions, ressources et clés de condition pour AWS Support
- Actions, ressources et clés de condition pour une AWS Support application dans Slack
- Actions, ressources et clés de condition pour AWS Support la console
- Actions, ressources et clés de condition pour les AWS Support plans
- Actions, ressources et clés de condition pour le AWS développement durable

- Actions, ressources et clés de condition pour AWS Systems Manager for SAP
- Actions, ressources et clés de condition pour AWS Systems Manager GUI Connect
- Actions, ressources et clés de condition pour AWS Systems Manager Incident Manager
- Actions, ressources et clés de condition pour les contacts de AWS Systems Manager Incident Manager
- Actions, ressources et clés de condition pour la configuration rapide de AWS Systems Manager
- Actions, ressources et clés de condition pour Tag Editor
- Actions, ressources et clés de condition pour les paramètres AWS fiscaux
- Actions, ressources et clés de condition pour AWS Telco Network Builder
- Actions, ressources et clés de condition pour Amazon Textract
- Actions, ressources et clés de condition pour Amazon Timestream
- Actions, ressources et clés de condition pour Amazon Timestream InfluxDB
- Actions, ressources et clés de condition pour AWS Tiros
- Actions, ressources et clés de condition pour Amazon Transcribe
- Actions, ressources et clés de condition pour AWS Transfer Family
- Actions, ressources et clés de condition pour AWS Transform
- Actions, ressources et clés de condition pour AWS Transform custom
- Actions, ressources et clés de condition pour Amazon Translate
- Actions, ressources et clés de condition pour AWS Trusted Advisor
- Actions, ressources et clés de condition pour la personnalisation de AWS l'expérience utilisateur
- Actions, ressources et clés de condition pour les notifications AWS utilisateur
- Actions, ressources et clés de condition pour les contacts relatifs aux notifications AWS utilisateur
- Actions, ressources et clés de condition pour les abonnements AWS utilisateur
- Actions, ressources et clés de condition pour l'accès AWS vérifié
- Actions, ressources et clés de condition pour Amazon Verified Permissions
- Actions, ressources et clés de condition pour Amazon VPC Lattice
- Actions, ressources et clés de condition pour les services Amazon VPC Lattice
- Actions, ressources et clés de condition pour AWS WAF
- Actions, ressources et clés de condition pour AWS WAF Regional
- Actions, ressources et clés de condition pour AWS WAF V2
- Actions, ressources et clés de condition pour AWS Well-Architected Tool

- Actions, ressources et clés de condition pour AWS Wickr
- Actions, ressources et clés de condition pour Amazon WorkDocs
- Actions, ressources et clés de condition pour Amazon WorkLink
- Actions, ressources et clés de condition pour Amazon WorkMail
- Actions, ressources et clés de condition pour Amazon WorkMail Message Flow
- Actions, ressources et clés de condition pour Amazon WorkSpaces
- Actions, ressources et clés de condition pour Amazon WorkSpaces Application Manager
- Actions, ressources et clés de condition pour les instances AWS WorkSpaces gérées
- Actions, ressources et clés de condition pour Amazon WorkSpaces Secure Browser
- Actions, ressources et clés de condition pour Amazon WorkSpaces Thin Client
- Actions, ressources et clés de condition pour AWS X-Ray

Actions, ressources et clés de condition pour la gestion des AWS comptes

AWS La gestion des comptes (préfixe de service :`account`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service de gestion des AWS comptes
- Types de ressources définis par la gestion des AWS comptes
- Clés de condition pour la gestion des AWS comptes

Actions définies par le service de gestion des AWS comptes

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptPrimaryEmailUpdate	Accorde l'autorisation d'accepter le processus de mise à jour de l'adresse e-mail principale d'un compte	Écrire	accountInOrganization		
				account:EmailTargetDomain	
CloseAccount [autorisation uniquement]	Accorde l'autorisation de fermer un compte	Écrire	account		
DeleteAlternateContact	Accorde l'autorisation de supprimer les autres contacts d'un compte	Écriture	account		
			accountInOrganization		
				account:AlternateContactTypes	
DisableRegion	Accorde l'autorisation de désactiver l'utilisation d'une région	Écrire	account		
			accountInOrganization		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				account:TargetRegion	
EnableRegion	Accorde l'autorisation d'activer l'utilisation d'une région	Écrire	account		
			accountInOrganization		
				account:TargetRegion	
GetAccountInformation	Accorde l'autorisation de récupérer les informations de compte pour un compte	Lecture	account		
			accountInOrganization		
GetAlternateContact	Accorde l'autorisation de récupérer les autres contacts d'un compte	Lecture	account		
			accountInOrganization		
				account:AlternateContactTypes	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContactInformation	Accorde l'autorisation de récupérer les informations de contact principal pour un compte	Lecture	account		
			accountInOrganization		
GetGovCloudAccountInformation	Accorde l'autorisation de récupérer les informations de GovCloud compte associées à un compte	Lecture	account		
			accountInOrganization		
GetPrimaryEmail	Accorde l'autorisation de récupérer l'adresse e-mail principale d'un compte	Lecture	accountInOrganization		
GetRegionOptStatus	Accorde l'autorisation d'obtenir le statut d'une vérification de l'état de préparation	Lecture	account		
			accountInOrganization		
				account:TargetRegion	
ListRegions	Accorde l'autorisation de répertorier les régions disponibles	List	account		
			accountInOrganization		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutAccountName	Accorde l'autorisation de mettre à jour le nom d'un compte	Écrire	account		
			accountInOrganization		
PutAlternateContact	Accorde l'autorisation de modifier les autres contacts d'un compte	Écrire	account		
			accountInOrganization		
				account:AlternateContactTypes	
PutContactInformation	Accorde l'autorisation de mettre à jour les informations de contact principal pour un compte	Écrire	account		
			accountInOrganization		
StartPrimaryEmailUpdate	Autorise le lancement du processus de mise à jour de l'adresse e-mail principale d'un compte	Écrire	accountInOrganization		
				account:EmailTargetDomain	

Types de ressources définis par la gestion des AWS comptes

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
account	`arn:${Partition}:account::${Account}:account`	
accountInOrganization	`arn:${Partition}:account::${ManagementAccountId}:account/o-${OrganizationId}/${MemberAccountId}`	

Clés de condition pour la gestion des AWS comptes

AWS La gestion des comptes définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
account:AccountResourceOrgPaths	Filtre l'accès par le chemin de ressources d'un compte d'une organisation	ArrayOfString
account:AccountRes	Filtre l'accès par les balises de ressources d'un compte d'une organisation	String

Clés de condition	Description	Type
ourceOrgTags/${TagKey}		
account:AlternateContactTypes	Filtre l'accès par d'autres types de contacts	ArrayOfString
account:EmailTargetDomain	Filtre l'accès par domaine de messagerie de l'adresse e-mail cible	String
account:TargetRegion	Filtre l'accès en fonction d'une liste de régions. Active ou désactive toutes les régions spécifiées ici	String

Actions, ressources et clés de condition pour les recommandations AWS d'action

AWS Les recommandations d'action (préfixe de service :`action-recommendations`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les recommandations AWS d'action
- Types de ressources définis par les recommandations AWS d'action
- Clés de condition pour les recommandations AWS d'action

Actions définies par les recommandations AWS d'action

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRecommendedActions	Accorde l'autorisation de répertorier les actions recommandées dans le AWS Management Console	List			

Types de ressources définis par les recommandations AWS d'action

AWS Action Recommendations ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès aux recommandations AWS d'action, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour les recommandations AWS d'action

Action Recommendations ne possède aucune clé de contexte spécifique à un service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Activate

AWS Activate (préfixe de service :`activate`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Activate
- Types de ressources définis par AWS Activate
- Clés de condition pour AWS Activate

Actions définies par AWS Activate

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateForm	Accorde l'autorisation de soumettre un formulaire de demande Activate	Écrire			
GetAccountContact	Accorde l'autorisation d'obtenir les informations de Compte AWS contact	Lecture			
GetContentInfo	Accorde l'autorisation d'obtenir les publications techniques	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Activate et d'offrir des informations				
GetCosts	Donne l'autorisation d'obtenir les informations sur les AWS coûts	Lecture			
GetCredits	Donne l'autorisation d'obtenir les informations AWS de crédit	Lecture			
GetMemberInfo	Accorde l'autorisation d'obtenir les informations sur un membre d'Activate	Lecture			
GetProgram	Accorde l'autorisation d'obtenir un programme Activate	Lecture			
PutMemberInfo	Accorde l'autorisation de créer ou de mettre à jour les informations sur un membre d'Activate	Écrire			

Types de ressources définis par AWS Activate

AWS Activate ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Activate, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Activate

Activate ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte

globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon AI Operations

Amazon AI Operations (préfixe de service :`aiops`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon AI Operations
- Types de ressources définis par Amazon AI Operations
- Clés de condition pour Amazon AI Operations

Actions définies par Amazon AI Operations

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInvestigation	Autorise la création d'une nouvelle enquête dans le groupe d'enquête spécifié	Écrire	investigation-group*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					kms:GenerateDataKey sts:SetContext

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInvestigationEvent	Autorise la création d'un nouvel événement d'enquête dans le groupe d'enquête spécifié	Écrire	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:Decrypt kms:GenerateDataKey logs:GetQueryResults sts:SetContext

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInvestigationGroup	Autorise la création d'un nouveau groupe de recherche	Écrire		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	aiops:TagResource cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInvestigationResource	Accorde l'autorisation de créer une ressource d'investigation dans le groupe d'investigation spécifié	Écrire	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:GenerateDataKey logs:GetQueryResults

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReport	Autorise la création d'un nouveau rapport dans le cadre de l'enquête spécifiée	Écrire	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
DeleteInvestigation	Autorise la suppression d'une enquête dans le groupe d'investigation spécifié	Écrire	investigation-group*		sts:SetContext
DeleteInvestigationGroup	Accorde l'autorisation de supprimer le groupe d'investigation spécifié	Écrire	investigation-group*		sso:DeleteApplication
DeleteInvestigationGroupPolicy	Accorde l'autorisation de supprimer la politique de groupe d'investigation attachée à un groupe d'enquête	Écrire	investigation-group*		
GenerateReport	Autorise la génération d'un rapport dans le rapport d'enquête spécifié	Écrire	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEphemeralInvestigationResults	Autorise l'exécution et la récupération de résultats d'enquêtes éphémères	List			
GetFact	Autorise la récupération d'un fait dans le rapport d'enquête spécifié	Lecture	investigation-group*		kms:Decrypt
GetFactVersions	Autorise la récupération de toutes les versions d'un fact-token dans le rapport d'enquête spécifié	Lecture	investigation-group*		kms:Decrypt
GetInvestigation	Accorde l'autorisation de récupérer une enquête dans le groupe d'enquête spécifié	Lecture	investigation-group*		
GetInvestigationEvent	Accorde l'autorisation de récupérer un événement d'enquête dans le groupe d'enquête spécifié	Lecture	investigation-group*		kms:Decrypt
GetInvestigationGroup	Accorde l'autorisation de récupérer le groupe d'investigation spécifié	Lecture	investigation-group*		
GetInvestigationGroupPolicy	Accorde l'autorisation de récupérer la politique du groupe d'enquête attachée à un groupe d'enquête	Lecture	investigation-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInvestigationResource	Accorde l'autorisation de récupérer une ressource d'investigation dans le groupe d'investigation spécifié	Lecture	investigation-group*		kms:Decrypt
GetReport	Accorde l'autorisation de récupérer un rapport dans le cadre de l'enquête spécifiée	Lecture	investigation-group*		kms:Decrypt
ListFacts	Permet d'énumérer tous les faits dans le rapport d'enquête spécifié	List	investigation-group*		kms:Decrypt
ListInvestigationEvents	Permet de répertorier tous les événements d'enquête du groupe d'enquête spécifié	List	investigation-group*		
ListInvestigationGroups	Autorise l'établissement de la liste de tous les groupes de recherche lors de la Compte AWS présentation de la demande	List			
ListInvestigations	Accorde l'autorisation de répertorier toutes les enquêtes appartenant au groupe d'enquête spécifié	List	investigation-group*		
ListReports	Permet de répertorier tous les rapports de l'enquête spécifiée	List	investigation-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée	List	investigation-group*		
PutFact	Autorise la création ou la mise à jour d'un nouveau fait dans le rapport d'enquête spécifié	Écrire	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
PutInvestigationGroupPolicy	Accorde l'autorisation à create/update la politique du groupe d'enquête attachée à un groupe d'enquête	Écrire	investigation-group*		
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour les balises spécifiées pour la ressource spécifiée	Identification	investigation-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de la ressource spécifiée	Identification	investigation-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateInvestigation	Autorise la mise à jour d'une enquête dans le groupe d'investigation spécifié	Écrire	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
UpdateInvestigationEvent	Autorise la mise à jour d'un événement d'enquête dans le groupe d'enquête spécifié	Écrire	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateInvestigationGroup	Autorise la mise à jour du groupe d'investigation spécifié	Écrire	investigation-group*		cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope sso:PutApplicationAssignmen

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					tConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource
UpdateReport	Autorise la mise à jour d'un rapport dans le cadre de l'enquête spécifiée	Écrire	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
ValidateInvestigationGroup	Accorde l'autorisation de valider le groupe d'investigation spécifié	Lecture	investigation-group*		

Types de ressources définis par Amazon AI Operations

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
investigation-group	`arn:${Partition}:aiops:${Region}:${Account}:investigation-group/${InvestigationGroupId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon AI Operations

Amazon AI Operations définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Alexa for Business

Alexa for Business (préfixe de service : `a4b`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Alexa for Business
- Types de ressources définis par Alexa for Business
- Clés de condition pour Alexa for Business

Actions définies par Alexa for Business

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApproveSkill	Accorde l'autorisation d'associer une compétence à l'organisation sous le nom du client Compte AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateContactWithAddressBook	Accorde l'autorisation d'associer un contact à un carnet d'adresses donné	Écriture	addressbook*		
			contact*		
AssociateDeviceWithNetworkProfile	Accorde l'autorisation d'associer un appareil au profil réseau spécifié	Écriture	device*		
			networkprofile*		
AssociateDeviceWithRoom	Accorde l'autorisation d'associer un appareil à une salle donnée	Écriture	device*		
			room*		
AssociateSkillGroupWithRoom	Accorde l'autorisation d'associer le groupe de compétences à une salle donnée	Écriture	room*		
			skillgroup*		
AssociateSkillWithSkillGroup	Accorde l'autorisation d'associer une compétence à un groupe de compétences	Écriture	skillgroup*		
AssociateSkillWithUsers	Accorde l'autorisation de mettre une compétence privée à la disposition des utilisateurs inscrits pour qu'ils l'activent sur leurs appareils	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CompleteRegistration [autorisation uniquement]	Accorde l'autorisation de terminer l'opération d'enregistrement d'un appareil Alexa	Écriture			
CreateAddressBook	Accorde l'autorisation de créer un carnet d'adresses avec les informations spécifiées	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBusinessReportSchedule	Accorde l'autorisation de créer une planification récurrente pour les rapports d'utilisation afin de fournir à l'emplacement S3 spécifié un intervalle quotidien ou hebdomadaire spécifique	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConferenceProvider	Accorde l'autorisation d'ajouter un nouveau fournisseur de conférence sous le nom de Compte AWS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateContact	Accorde l'autorisation de créer un contact avec les informations spécifiées	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGatewayGroup	Accorde l'autorisation de créer un groupe de passerelles avec les informations spécifiées	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkProfile	Accorde l'autorisation de créer un profil réseau avec les informations spécifiées	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Accorde l'autorisation de créer un nouveau profil	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoom	Accorde l'autorisation de créer une salle avec les informations spécifiées	Écriture	profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSkillGroup	Accorde l'autorisation de créer un groupe de compétences avec un nom et une description donnés	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Accorde l'autorisation de créer un utilisateur	Écriture	user*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddressBook	Accorde l'autorisation de supprimer un carnet d'adresses à partir de l'ARN de celui-ci	Écriture	addressbook*		
DeleteBusinessReportSchedule	Accorde l'autorisation de supprimer le programme d'envoi de rapport récurrent avec l'ARN du programme spécifié	Écriture	schedule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConferenceProvider	Accorde l'autorisation de supprimer un fournisseur de conférence	Écriture	conferenceprovider*		
DeleteContact	Accorde l'autorisation de supprimer un contact à partir de l'ARN de celui-ci	Écriture	contact*		
DeleteDevice	Accorde l'autorisation de supprimer un appareil d'Alexa For Business	Écriture	device*		
DeleteDeviceUsageData	Accorde l'autorisation de supprimer de l'appareil l'intégralité de l'historique des entrées vocales et des réponses associées	Écriture	device*		
DeleteGatewayGroup	Accorde l'autorisation de supprimer un groupe de passerelles	Écriture	gatewaygroup*		
DeleteNetworkProfile	Accorde l'autorisation de supprimer un profil réseau à partir de l'ARN de celui-ci	Écriture	networkprofile*		
DeleteProfile	Accorde l'autorisation de supprimer un profil à partir de l'ARN de celui-ci	Écriture	profile*		
DeleteRoom	Accorde l'autorisation de supprimer une salle	Écriture	room*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRoomSkillParameter	Accorde l'autorisation de supprimer un paramètre d'une compétence et d'une salle	Écriture	room*		
DeleteSkillAuthorization	Accorde l'autorisation de dissocier un compte tiers d'une compétence	Écriture	room*		
DeleteSkillGroup	Accorde l'autorisation de supprimer un groupe de compétences à partir de l'ARN de celui-ci	Écriture	skillgroup*		
DeleteUser	Accorde l'autorisation de supprimer un utilisateur	Écriture	user*		
DisassociateContactFromAddressBook	Accorde l'autorisation de dissocier un contact d'un carnet d'adresses donné	Écriture	addressbook*		
			contact*		
DisassociateDeviceFromRoom	Accorde l'autorisation de dissocier l'appareil de sa salle actuelle	Écriture	device*		
DisassociateSkillFromSkillGroup	Accorde l'autorisation de dissocier une compétence d'un groupe de compétences	Écriture	skillgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateSkillFromUsers	Accorde l'autorisation de rendre une compétence privée indisponible pour les utilisateurs inscrits afin de les empêcher de l'activer sur leurs appareils	Écriture	user*		
DisassociateSkillGroupFromRoom	Accorde l'autorisation de dissocier le groupe de compétences de la salle donnée	Écriture	room* skillgroup*		
ForgetSmartHomeAppliances	Accorde l'autorisation d'omettre des appareils électroménagers intelligents associés à une salle	Écriture	room*		
GetAddressBook	Accorde l'autorisation de récupérer les informations du carnet d'adresses à partir de l'ARN de celui-ci	Lecture	addressbook*		
GetConferencePreference	Accorde l'autorisation de récupérer les préférences de conférence existantes	Lecture			
GetConferenceProvider	Accorde l'autorisation de récupérer les informations relatives à un fournisseur de conférence spécifique	Lecture	conferenceprovider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContact	Accorde l'autorisation de récupérer les coordonnées d'un contact partir de son ARN	Lecture	contact*		
GetDevice	Accorde l'autorisation de récupérer les informations relatives à un appareil	Lecture	device*		
GetGateway	Accorde l'autorisation de récupérer les informations relatives à une passerelle	Lecture	gateway*		
GetGatewayGroup	Accorde l'autorisation de récupérer les informations relatives à un groupe de passerelles	Lecture	gatewaygroup*		
GetInvitationConfiguration	Accorde l'autorisation de récupérer les valeurs configurées pour le modèle d'e-mail d'invitation à l'inscription de l'utilisateur	Lecture			
GetNetworkProfile	Accorde l'autorisation de récupérer les informations relatives au profil réseau à partir de l'ARN de celui-ci	Lecture	networkprofile*		
GetProfile	Accorde l'autorisation de récupérer le profil, lorsqu'il est fourni, à partir de l'ARN de celui-ci	Lecture	profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRoom	Accorde l'autorisation de récupérer les informations relatives à la salle	Lecture	room*		
GetRoomSkillParameter	Accorde l'autorisation de récupérer un paramètre existant qui a été défini pour une compétence et une salle	Lecture	room*		
GetSkillGroup	Accorde l'autorisation de récupérer les informations relatives à un groupe de compétences à partir de l'ARN de celui-ci	Lecture	skillgroup*		
ListBusinessReportSchedules	Accorde l'autorisation de récupérer les informations relatives aux planifications configurées par un utilisateur	List			
ListConferenceProviders	Permet de répertorier les fournisseurs de conférences sous un nom spécifique Compte AWS	List			
ListDeviceEvents	Accorde l'autorisation de répertorier l'historique des événements d'un appareil, y compris l'état de la connexion de l'appareil, pour une durée maximale de 30 jours	Liste	device*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGatewayGroups	Accorde l'autorisation de répertorier les récapitulatifs des groupes de passerelles	Liste			
ListGateways	Accorde l'autorisation de répertorier les récapitulatifs des passerelles	Liste	gatewaygroup*		
ListSkills	Accorde l'autorisation de répertorier les compétences	Liste			
ListSkillsStoreCategories	Accorde l'autorisation de répertorier toutes les catégories de la boutique de compétences Alexa	Liste			
ListSkillsStoreSkillsByCategory	Accorde l'autorisation de répertorier toutes les compétences de la boutique de compétences Alexa, par catégorie	Liste			
ListSmartHomeAppliances	Accorde l'autorisation de répertorier tous les appareils électroménagers intelligents associés à une salle	Liste	room*		
ListTags	Accorde l'autorisation de répertorier toutes les balises d'une ressource	Lecture	device		
			room		
			user		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutConferencePreference	Accorde l'autorisation de définir les préférences de conférence sur un fournisseur de conférence spécifique au niveau du compte	Écriture			
PutDeviceSetupEvents [autorisation uniquement]	Accorde l'autorisation de publier les événements de configuration d'un appareil Alexa	Écriture			
PutInvitationConfiguration	Accorde l'autorisation de configurer le modèle d'e-mail d'invitation à l'inscription de l'utilisateur avec les attributs spécifiés	Écriture			
PutRoomSkillParameter	Accorde l'autorisation d'insérer un paramètre spécifique à la salle pour une compétence	Écriture	room*		
PutSkillAuthorization	Accorde l'autorisation de créer un lien entre le compte d'un utilisateur à un fournisseur de compétences tiers	Écriture	room*		
RegisterAVSDevice	Accorde l'autorisation d'enregistrer un appareil compatible Alexa créé par un fabricant OEM en utilisant Alexa Voice Service (AVS)	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterDevice [autorisation uniquement]	Accorde l'autorisation d'enregistrer un appareil Alexa	Écrire			
RejectSkill	Accorde l'autorisation de dissocier une compétence de l'organisation sous celle d'un utilisateur Compte AWS	Écrire			
ResolveRoom	Accorde l'autorisation de résoudre les informations de la salle	Lecture			
RevokeInvitation	Accorde l'autorisation d'annuler une invitation	Écriture	user*		
SearchAddressBooks	Accorde l'autorisation de rechercher des carnets d'adresses et de répertorier ceux qui répondent à un ensemble de critères de filtrage et de tri	Liste			
SearchContacts	Accorde l'autorisation de rechercher des contacts et de répertorier ceux qui répondent à un ensemble de critères de filtrage et de tri	Liste			
SearchDevices	Accorde l'autorisation de rechercher des appareils	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchNetworkProfiles	Accorde l'autorisation de rechercher des profils réseau et de répertorier ceux qui répondent à un ensemble de critères de filtrage et de tri	Liste			
SearchProfiles	Accorde l'autorisation de rechercher des profils	Liste			
SearchRooms	Accorde l'autorisation de rechercher des salles	Liste			
SearchSkillGroups	Accorde l'autorisation de rechercher des groupes de compétences	Liste			
SearchUsers	Accorde l'autorisation de rechercher des utilisateurs	Liste			
SendAnnouncement	Accorde l'autorisation de déclencher un flux asynchrone pour envoyer des annonces textuelles, SSML ou audio aux salles identifiées par une recherche ou un filtre	Écriture			
SendInvitation	Accorde l'autorisation d'envoyer une invitation à un utilisateur	Écriture	user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDeviceSync	Accorde l'autorisation de restaurer les paramètres par défaut connus d'un appareil et de son compte en effaçant toutes les informations et tous les paramètres définis par ses utilisateurs précédents	Écriture			
StartSmartHomeApplianceDiscovery	Accorde l'autorisation de démarrer la recherche des appareils électroménagers intelligents associés à la salle	Lecture	room*		
TagResource	Accorde l'autorisation d'ajouter des balises de métadonnées à une ressource	Balisage	device		
			room		
			user		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises de métadonnées d'une ressource	Balisage	device		
			room		
			user		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAddressBook	Accorde l'autorisation de mettre à jour les informations du carnet d'adresses à partir de l'ARN de celui-ci	Écriture	addressbook*		
UpdateBusinessReportSchedule	Accorde l'autorisation de mettre à jour la configuration du programme d'envoi de rapports à partir de l'ARN de celui-ci	Écriture	schedule*		
UpdateConferenceProvider	Accorde l'autorisation de mettre à jour les paramètres d'un fournisseur de conférence existant	Écriture	conferenceprovider*		
UpdateContact	Accorde l'autorisation de mettre à jour les coordonnées d'un contact à partir de son ARN	Écriture	contact*		
UpdateDevice	Accorde l'autorisation de mettre à jour le nom d'un appareil	Écriture	device*		
UpdateGateway	Accorde l'autorisation de mettre à jour les informations relatives à une passerelle	Écriture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGatewayGroup	Accorde l'autorisation de mettre à jour les informations relatives à un groupe de passerelles	Écriture	gatewaygroup*		
UpdateNetworkProfile	Accorde l'autorisation de mettre à jour un profil réseau à partir de l'ARN de celui-ci	Écriture	networkprofile*		
UpdateProfile	Accorde l'autorisation de mettre à jour un profil existant	Écriture	profile*		
UpdateRoom	Accorde l'autorisation de mettre à jour les informations relatives à une salle	Écriture	room*		
UpdateSkillGroup	Accorde l'autorisation de mettre à jour les informations relatives à un groupe de compétences à partir de l'ARN de celui-ci	Écriture	skillgroup*		

Types de ressources définis par Alexa for Business

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
profile	arn:${Partition}:a4b:${Region}:${Account}:profile/${ResourceId}	
room	arn:${Partition}:a4b:${Region}:${Account}:room/${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:a4b:${Region}:${Account}:device/${ResourceId}	aws:ResourceTag/${TagKey}
skillgroup	arn:${Partition}:a4b:${Region}:${Account}:skill-group/${ResourceId}	
user	arn:${Partition}:a4b:${Region}:${Account}:user/${ResourceId}	aws:ResourceTag/${TagKey}
addressbook	arn:${Partition}:a4b:${Region}:${Account}:address-book/${ResourceId}	
conferenceprovider	arn:${Partition}:a4b:${Region}:${Account}:conference-provider/${ResourceId}	
contact	arn:${Partition}:a4b:${Region}:${Account}:contact/${ResourceId}	
schedule	arn:${Partition}:a4b:${Region}:${Account}:schedule/${ResourceId}	
networkprofile	arn:${Partition}:a4b:${Region}:${Account}:network-profile/${ResourceId}	
gateway	arn:${Partition}:a4b:${Region}:${Account}:gateway/${ResourceId}	
gatewaygroup	arn:${Partition}:a4b:${Region}:${Account}:gateway-group/${ResourceId}	

Clés de condition pour Alexa for Business

Alexa for Business définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
a4b:amazonId	Filtre les actions en fonction de l'ID Amazon figurant dans la demande.	Chaîne
a4b:filters_deviceType	Filtre les actions en fonction du type d'appareil dans la demande.	ArrayOfString
aws:RequestTag/${TagKey}	Filtre les actions en fonction de l'ensemble des valeurs autorisées pour chacune des balises.	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur de balise associé à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AmazonMediaImport

AmazonMediaImport (préfixe de service :`mediaimport`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AmazonMediaImport
- Types de ressources définis par AmazonMediaImport
- Clés de condition pour AmazonMediaImport

Actions définies par AmazonMediaImport

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDatabaseBinarySnapshot [autorisation uniquement]	Accorde l'autorisation de créer un instantané binaire de base de données sur le compte AWS du client	Écrire			

Types de ressources définis par AmazonMediaImport

AmazonMediaImport ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AmazonMediaImport, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AmazonMediaImport

mediaimport ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Amplify

AWS Amplify (préfixe de service :`amplify`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Amplify
- Types de ressources définis par AWS Amplify
- Clés de condition pour AWS Amplify

Actions définies par AWS Amplify

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateWebACL	Accorde l'autorisation d'associer un WebACL à une ressource	Écrire	apps*		
CreateApp	Accorde l'autorisation de créer une nouvelle application Amplify	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackendEnvironment	Accorde l'autorisation de créer un nouvel environnement backend pour une application Amplify	Écrire	apps*		
CreateBranch	Accorde l'autorisation de créer une nouvelle branche pour une application Amplify	Écrire	branches*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeployment	Accorde l'autorisation de créer un déploiement manuel pour le déploiement manuel d'applications. (Les applications ne sont pas connectées au référentiel)	Écrire	branches*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDomainAssociation	Accorde l'autorisation d'en créer un nouveau DomainAssociation sur une application	Écrire	domains*		
CreateWebHook	Accorde l'autorisation de créer un nouveau webhook sur une application	Écrire	branches*		
DeleteApp	Accorde l'autorisation pour supprimer une application Amplify existante par appId	Écrire	apps*		
DeleteBackendEnvironment	Accorde l'autorisation de supprimer une branche pour une application Amplify	Écrire	apps*		
DeleteBranch	Accorde l'autorisation de supprimer une branche pour une application Amplify	Écrire	branches*		
DeleteDomainAssociation	Accorde l'autorisation de supprimer un DomainAssociation	Écrire	domains*		
DeleteJob	Accorde l'autorisation de supprimez une tâche, pour une branche Amplify, partie intégrante d'une application Amplify	Écrire	jobs*		
DeleteWebHook	Accorde l'autorisation de supprimer un webhook par id	Écrire	webhooks*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateWebACL	Accorde l'autorisation de dissocier un WebACL d'une ressource	Écrire	apps*		
GenerateAccessLogs	Accorde l'autorisation de générer des journaux d'accès pour une plage de temps spécifique via une URL présignée	Écrire	apps*		
GetApp	Accorde l'autorisation de récupérer une application Amplify existante par appId.	Lecture	apps*		
GetArtifactUrl	Accorde l'autorisation de récupérer les informations d'artefact qui correspondent à un artefactId	Lecture	apps*		
GetBackendEnvironment	Accorde l'autorisation de récupérer un environnement backend pour une application Amplify	Lecture	apps*		
GetBranch	Accorde l'autorisation de récupérer une branche pour une application Amplify	Lecture	branches*		
GetDomainAssociation	Accorde l'autorisation de récupérer les informations de domaine correspondant à un appId et un domainName	Lecture	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetJob	Accorde l'autorisation d'obtenir une tâche pour une branche, partie d'une application Amplify	Lecture	jobs*		
GetWebACLForResource	Accorde l'autorisation de récupérer le WebACL associé à une ressource	Lecture	apps*		
GetWebHook	Accorde l'autorisation de récupèrer les informations de webhook qui correspondent à un webhookId	Lecture	webhooks*		
ListApps	Accorde l'autorisation de répertorier les applications Amplify existantes	List			
ListArtifacts	Accorde l'autorisation de répertorier des artefacts avec une application, une branche, une tâche et un type d'artefact	List	apps*		
ListBackendEnvironments	Accorde l'autorisation de répertorier les environnements backend d'une application Amplify	List	apps*		
ListBranches	Accorde l'autorisation de répertorier les branches pour une application Amplify	List	apps*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDomainAssociations	Accorde l'autorisation de répertorier les domaines avec une application	List	apps*		
ListJobs	Accorde l'autorisation de répertorier les tâches pour une branche, partie d'une application Amplify	List	branches*		
ListResourcesForWebACL	Accorde l'autorisation de répertorier les ressources associées à un WebACL	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource AWS Amplify Console	Lecture	apps		
			branches		
			domains		
			webhooks		
ListWebHooks	Accorde l'autorisation de répertorier les webhooks sur une application	List	apps*		
StartDeployment	Accorde l'autorisation de démarrer un déploiement pour les applications de déploiement manuel. (Les applications ne sont pas connectées au référentiel)	Écrire	branches*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartJob	Accorde l'autorisation de démarrer une nouvelle tâche pour une branche, partie d'une application Amplify	Écrire	jobs*		
StopJob	Accorde l'autorisation d'arrêter une tâche qui est en cours, pour une branche Amplify, partie d'une application Amplify	Écrire	jobs*		
TagResource	Accorde l'autorisation de baliser une AWS ressource Amplify Console	Identification	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource AWS Amplify Console	Identification	apps		
			branches		
			domains		
			webhooks		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateApp	Accorde l'autorisation pour mettre à jour une application Amplify existante	Écrire	apps*		
UpdateBranch	Accorde l'autorisation de mettre à jour une branche pour une application Amplify	Écrire	branches*		
UpdateDomainAssociation	Accorde l'autorisation de mettre à jour un DomainAssociation sur une application	Écrire	domains*		
UpdateWebHook	Accorde l'autorisation de mettre à jour un webhook	Écrire	webhooks*		

Types de ressources définis par AWS Amplify

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
apps	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}	aws:ResourceTag/${TagKey}
branches	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}	aws:ResourceTag/${TagKey}
jobs	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}/jobs/${JobId}	
domains	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/domains/${DomainName}	aws:ResourceTag/${TagKey}
webhooks	arn:${Partition}:amplify:${Region}:${Account}:webhooks/${WebhookId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Amplify

AWS Amplify définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des clés d'identification associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Amplify Admin

AWS Amplify Admin (préfixe de service :`amplifybackend`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Amplify Admin
- Types de ressources définis par AWS Amplify Admin
- Clés de condition pour AWS Amplify Admin

Actions définies par AWS Amplify Admin

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CloneBackend	Accorde l'autorisation de cloner un environnement backend Amplify Admin existant dans un nouvel environnement backend Amplify Admin	Écriture	backend*		
CreateBackend	Accorde l'autorisation de créer un nouvel environnement backend Amplify Admin par Amplify appId	Écrire	created-backend*		
CreateBackendAPI	Accorde l'autorisation de créer une API pour un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Écrire	api*		
			backend*		
			environment*		
CreateBackendAuth	Accorde l'autorisation de créer une ressource d'authentification pour un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Écrire	auth*		
			backend*		
			environment*		
CreateBackendConfig	Accorde l'autorisation de créer une nouvelle configuration backend Amplify Admin par Amplify appId	Écrire	config*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBackendStorage	Accorde l'autorisation de créer une ressource de stockage backend	Écrire	backend*		
			environment*		
			storage*		
CreateToken	Accorde l'autorisation de créer un jeton de stimulation Amplify Admin par appId	Écrire	backend*		
			token*		
DeleteBackend	Accorde l'autorisation de supprimer un environnement de backend Amplify Admin existant par AppID et backendEnvironmentName	Écrire	backend*		
			environment*		
DeleteBackendAPI	Accorde l'autorisation de supprimer une API d'un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Écrire	api*		
			backend*		
			environment*		
DeleteBackendAuth	Accorde l'autorisation de supprimer une ressource d'authentification d'un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Écrire	auth*		
			backend*		
			environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBackendStorage	Accorde l'autorisation de supprimer une ressource de stockage backend	Écrire	backend*		
			environment*		
			storage*		
DeleteToken	Accorde l'autorisation de supprimer un jeton de stimulation Amplify Admin par appId	Écrire	backend*		
			token*		
GenerateBackendAPIModels	Accorde l'autorisation de générer des modèles pour une API d'un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Écrire	api*		
			backend*		
			environment*		
GetBackend	Accorde l'autorisation de récupérer un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Lecture	backend*		
			environment*		
GetBackendAPI	Accorde l'autorisation de récupérer une API d'un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Lecture	api*		
			backend*		
			environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBackendAPIModels	Accorde l'autorisation de récupérer des modèles pour une API d'un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Lecture	api*		
			backend*		
			environment*		
GetBackendAuth	Accorde l'autorisation de récupérer une ressource d'authentification d'un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Lecture	auth*		
			backend*		
			environment*		
GetBackendJob	Accorde l'autorisation de récupérer une tâche d'un environnement backend Amplify Admin existant par AppID et backendEnvironmentName	Lecture	backend*		
			job*		
GetBackendStorage	Accorde l'autorisation de récupérer une ressource de stockage backend existante	Lecture	backend*		
			environment*		
GetToken	Accorde l'autorisation de récupérer un jeton de stimulation Amplify Admin par appId	Lecture	backend*		
			token*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportBackendAuth	Accorde l'autorisation d'importer une ressource d'authentification existante d'un environnement de backend Amplify Admin par AppID et backendEnvironment Name	Écrire	auth*		
			backend*		
			environment*		
ImportBackendStorage	Accorde l'autorisation d'importer une ressource de stockage backend existante	Écrire	backend*		
			environment*		
			storage*		
ListBackendJobs	Accorde l'autorisation de récupérer les tâches d'un environnement backend Amplify Admin existant par AppID et backendEnvironment Name	List	backend*		
			job*		
ListS3Buckets	Accorde l'autorisation de récupérer des compartiments s3	List			s3:ListAllMyBuckets
RemoveAllBackends	Accorde l'autorisation de supprimer tous les environnements backend Amplify Admin existants par appId	Écriture	backend*		
			environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveBackendConfig	Accorde l'autorisation de supprimer une configuration backend Amplify Admin par Amplify appId	Écrire	config*		
UpdateBackendAPI	Accorde l'autorisation de mettre à jour une API d'un environnement backend Amplify Admin existant par AppID et backendEnvironment Name	Écrire	api*		
			backend*		
			environment*		
UpdateBackendAuth	Accorde l'autorisation de mettre à jour une ressource d'authentification d'un environnement backend Amplify Admin existant par AppID et backendEnvironment Name	Écrire	auth*		
			backend*		
			environment*		
UpdateBackendConfig	Accorde l'autorisation de mettre à jour une configuration backend Amplify Admin par Amplify appId	Écrire	config*		
UpdateBackendJob	Accorde l'autorisation de mettre à jour une tâche d'un environnement backend Amplify Admin existant par AppID et backendEnvironment Name	Écrire	backend*		
			job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateBackendStorage	Accorde l'autorisation de mettre à jour une ressource de stockage backend	Écrire	backend*		
			environment*		
			storage*		

Types de ressources définis par AWS Amplify Admin

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
created-backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/*`	
backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/*`	
environment	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/environments/*`	

Types de ressources	ARN	Clés de condition
api	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/api/*`	
auth	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/auth/*`	
job	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/job/*`	
config	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/config/*`	
token	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/challenge/*`	
storage	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/storage/*`	

Clés de condition pour AWS Amplify Admin

Amplify Admin ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Amplify UI Builder

AWS Amplify UI Builder (préfixe de service :`amplifyuibuilder`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Amplify UI Builder
- Types de ressources définis par AWS Amplify UI Builder
- Clés de condition pour AWS Amplify UI Builder

Actions définies par AWS Amplify UI Builder

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateComponent	Accorde l'autorisation de créer un composant	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:G

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					etComponent amplifyuibuilder:TagResource
CreateForm	Accorde l'autorisation de créer un formulaire	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTheme	Accorde l'autorisation de créer un thème	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource
DeleteComponent	Accorde l'autorisation de supprimer un composant	Écrire	ComponentResource*		amplify:GetApp amplifyuibuilder:UntagResource
DeleteForm	Accorde l'autorisation de supprimer un formulaire	Écrire	FormResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTheme	Accorde l'autorisation de supprimer un thème.	Écrire	ThemeResource*		amplify:GetApp amplifyuibuilder:UntagResource
ExchangeCodeForToken	Accorde l'autorisation d'échanger un code contre un jeton	Écrire			
ExportComponents	Accorde l'autorisation d'exporter des composants	Lecture			
ExportForms	Accorde l'autorisation d'exporter des formulaires	Lecture			
ExportThemes	Accorde l'autorisation d'exporter des thèmes	Lecture			
GetCodegenJob	Accorde l'autorisation d'obtenir une tâche de génération de code existante	Lecture	CodegenJobResource*		amplify:GetApp
GetComponent	Accorde l'autorisation d'obtenir un composant existant	Lecture	ComponentResource*		amplify:GetApp
GetForm	Accorde l'autorisation d'obtenir un formulaire existant	Lecture	FormResource*		amplify:GetApp
GetMetadata	Accorde l'autorisation d'obtenir une métadonnée existante	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTheme	Accorde l'autorisation d'obtenir un thème existant	Lecture	ThemeResource*		amplify:GetApp
ListCodegenJobs	Accorde l'autorisation de répertorier les tâches de génération de code	List			amplify:GetApp
ListComponents	Accorde l'autorisation de répertorier les composants	List			amplify:GetApp
ListForms	Accorde l'autorisation de répertorier des formulaires	List			amplify:GetApp
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour un Amazon Resource Name (ARN) spécifié	List	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
ListThemes	Accorde l'autorisation de répertorier des thèmes	List			amplify:GetApp
PutMetadataFlag	Accorde l'autorisation de placer une métadonnée existante	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RefreshToken	Accorde l'autorisation d'actualiser un jeton d'accès	Écrire			
ResetMetadataFlag	Accorde l'autorisation de réinitialiser une métadonnée existante	Écrire			
StartCodegenJob	Accorde l'autorisation de démarrer une tâche de génération de code	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp
TagResource	Accorde l'autorisation de baliser la ressource avec une clé et une valeur de balise	Identification	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource avec un Amazon Resource Name (ARN) spécifié	Identification	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys	
UpdateComponent	Accorde l'autorisation de mettre à jour un composant	Écrire	ComponentResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateForm	Accorde l'autorisation de mettre à jour un formulaire	Écrire	FormResource*		amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTheme	Accorde l'autorisation de mettre à jour un thème	Écrire	ThemeResource*		amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Types de ressources définis par AWS Amplify UI Builder

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
CodegenJobResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/codegen-jobs/${Id}	amplifyuibuilder:CodegenJobResourceAppId amplifyuibuilder:CodegenJobResourceEnvironmentName amplifyuibuilder:CodegenJobResourceId aws:ResourceTag/${TagKey}
ComponentResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/components/${Id}	amplifyuibuilder:ComponentResourceAppId amplifyuibuilder:ComponentResourceEnvironmentName amplifyuibuilder:ComponentResourceId aws:ResourceTag/${TagKey}
FormResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/forms/${Id}	amplifyuibuilder:FormResourceAppId amplifyuibuilder:FormResourceEnvironmentName

Types de ressources	ARN	Clés de condition
		amplifyuibuilder:FormResourceId aws:ResourceTag/${TagKey}
ThemeResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/themes/${Id}	amplifyuibuilder:ThemeResourceAppId amplifyuibuilder:ThemeResourceEnvironmentName amplifyuibuilder:ThemeResourceId aws:ResourceTag/${TagKey}

Clés de condition pour AWS Amplify UI Builder

AWS Amplify UI Builder définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
amplifyuibuilder:CodegenJobResourceAppId	Filtre l'accès en fonction de l'ID d'application	String

Clés de condition	Description	Type
amplifyuibuilder:CodegenJobResourceEnvironmentName	Filtre l'accès en fonction du nom d'environnement backend	String
amplifyuibuilder:CodegenJobResourceId	Filtre l'accès en fonction de l'ID de la tâche de génération de code	String
amplifyuibuilder:ComponentResourceAppId	Filtre l'accès en fonction de l'ID d'application	String
amplifyuibuilder:ComponentResourceEnvironmentName	Filtre l'accès en fonction du nom d'environnement backend	String
amplifyuibuilder:ComponentResourceId	Filtre l'accès en fonction de l'ID du composant	String
amplifyuibuilder:FormResourceAppId	Filtre l'accès en fonction de l'ID d'application	String

Clés de condition	Description	Type
amplifyuibuilder:FormResourceEnvironmentName	Filtre l'accès en fonction du nom d'environnement backend	String
amplifyuibuilder:FormResourceId	Filtre l'accès en fonction de l'ID du formulaire	String
amplifyuibuilder:ThemeResourceAppId	Filtre l'accès en fonction de l'ID d'application	String
amplifyuibuilder:ThemeResourceEnvironmentName	Filtre l'accès en fonction du nom d'environnement backend	String
amplifyuibuilder:ThemeResourceId	Filtre l'accès en fonction de l'ID du thème	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les clusters Apache Kafka APIs pour Amazon MSK

Apache Kafka APIs pour les clusters Amazon MSK (préfixe de service :`kafka-cluster`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Apache Kafka APIs pour les clusters Amazon MSK
- Types de ressources définis par Apache Kafka APIs pour les clusters Amazon MSK
- Clés de condition pour les clusters Apache Kafka APIs pour Amazon MSK

Actions définies par Apache Kafka APIs pour les clusters Amazon MSK

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AlterCluster	Autorise la modification de divers aspects du cluster, équivalent à l'ACL ALTER CLUSTER d'Apache Kafka.	Écriture	cluster*		kafka-cluster:Connect

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					kafka-cluster:DescribeCluster
AlterClusterDynamicConfiguration	Autorise la modification de la configuration dynamique d'un cluster, équivalente à l'ACL ALTER_CONFIGS CLUSTER d'Apache Kafka.	Écriture	cluster*		kafka-cluster:Connect kafka-cluster:DescribeClusterDynamicConfiguration
AlterGroup	Autorise la participation à des groupes sur un cluster, équivalent à l'ACL READ GROUP d'Apache Kafka.	Écriture	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
AlterTopic	Autorise la modification de rubriques dans un cluster, équivalent à l'ACL ALTER TOPIC d'Apache Kafka.	Écriture	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AlterTopicDynamicConfiguration	Autorise la modification de la configuration dynamique des rubriques dans un cluster, équivalent à l'ACL ALTER_CONFIGS TOPIC d'Apache Kafka.	Écrire	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamicConfiguration
AlterTransactionalId	Accorde l'autorisation de modifier les transactions IDs sur un cluster, ce qui est équivalent à l'ACL WRITE TRANSACTIONAL_ID d'Apache Kafka	Écrire	transactional-id*		kafka-cluster:Connect kafka-cluster:DescribeTransactionalId kafka-cluster:WriteData
Connect	Autorise la connexion et l'authentification dans un cluster.	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTopic	Accorde l'autorisation de créer des sujets sur un cluster, équivalent à l'ACL CREATE CLUSTER/TOPIC d'Apache Kafka	Écrire	topic*		kafka-cluster:Connect
DeleteGroup	Autorise la suppression des groupes d'un cluster, équivalent à l'ACL DELETE GROUP d'Apache Kafka.	Écriture	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
DeleteTopic	Autorise la suppression des rubriques dans un cluster, équivalent à l'ACL DELETE TOPIC d'Apache Kafka.	Écriture	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
DescribeCluster	Autorise la description de divers aspects du cluster, équivalent à l'ACL DESCRIBE CLUSTER d'Apache Kafka.	Liste	cluster*		kafka-cluster:Connect
DescribeClusterDynamicConfiguration	Autorise la description de la configuration dynamique d'un cluster, équivalent à l'ACL DESCRIBE_CONFIGS CLUSTER d'Apache Kafka.	Liste	cluster*		kafka-cluster:Connect

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGroup	Autorise la description des groupes sur un cluster, équivalent à l'ACL DESCRIBE GROUP d'Apache Kafka.	Liste	group*		kafka-cluster:Connect
DescribeTopic	Autorise la description des rubriques dans un cluster, équivalent à l'ACL DESCRIBE TOPIC d'Apache Kafka.	Liste	topic*		kafka-cluster:Connect
DescribeTopicDynamicConfiguration	Autorise la description de la configuration dynamique des rubriques dans un cluster, équivalent à l'ACL DESCRIBE_CONFIGS TOPIC d'Apache Kafka.	List	topic*		kafka-cluster:Connect
DescribeTransactionalId	Accorde l'autorisation de décrire les transactions IDs sur un cluster, ce qui est équivalent à l'ACL DESCRIBE TRANSACTIONAL_ID d'Apache Kafka	List	transactional-id*		kafka-cluster:Connect

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ReadData	Autorise la lecture des données provenant de rubriques dans un cluster, équivalent à l'ACL READ TOPIC d'Apache Kafka.	Lecture	topic*		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData	Autorise l'écriture des données dans les rubriques d'un cluster, équivalent à l'ACL WRITE TOPIC d'Apache Kafka.	Écriture	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteData Idempotently	Autorise l'écriture des données de manière idempotente dans un cluster, équivalent à l'ACL IDEMPOTENT_WRITE CLUSTER d'Apache Kafka.	Écrire	cluster*		kafka-cluster:Connect kafka-cluster:WriteData

Types de ressources définis par Apache Kafka APIs pour les clusters Amazon MSK

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${ClusterUuid}`	aws:ResourceTag/${TagKey}
topic	`arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}`	
group	`arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}`	
transactional-id	`arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}`	

Clés de condition pour les clusters Apache Kafka APIs pour Amazon MSK

Apache Kafka APIs pour les clusters Amazon MSK définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur de balise attachées à la ressource. La clé de contexte de la balise de ressource ne s'appliquera qu'à la ressource du cluster, et non aux sujets, aux groupes et aux transactions IDs	String

Actions, ressources et clés de condition pour Amazon API Gateway

Amazon API Gateway (préfixe de service : `execute-api`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon API Gateway
- Types de ressources définis par Amazon API Gateway
- Clés de condition pour Amazon API Gateway

Actions définies par Amazon API Gateway

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvalidateCache	Accorde l'autorisation d'invalider le cache d'API à la demande d'un client	Écrire	execute-api-general*		
Invoke	Accorde l'autorisation d'invoquer une API à la demande d'un client	Écrire	execute-api-domain		
			execute-api-general		
ManageConnections	Accorde l'autorisation d'accéder à la route Websocket @connections	Écrire	execute-api-general*		

Types de ressources définis par Amazon API Gateway

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
execute-api-general	`arn:${Partition}:execute-api:${Region}:${Account}:${ApiId}/${Stage}/${Method}/${ApiSpecificResourcePath}`	execute-api:viaDomainArn
execute-api-domain	`arn:${Partition}:execute-api:${Region}:${Account}:/domainnames/${DomainName}+${DomainIdentifier}`	

Clés de condition pour Amazon API Gateway

Amazon API Gateway définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
execute-api:viaDomainArn	Filtre l'accès par l' DomainName ARN à partir duquel l'API est appelée	ARN

Actions, ressources et clés de condition pour AWS App Mesh

AWS App Mesh (préfixe de service :`appmesh`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS App Mesh
- Types de ressources définis par AWS App Mesh
- Clés de condition pour AWS App Mesh

Actions définies par AWS App Mesh

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGatewayRoute	Accorde l'autorisation de créer une route de passerelle associée à une passerelle virtuelle	Écriture	gatewayRoute*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateMesh	Accorde l'autorisation de créer un maillage de services	Écriture	mesh*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRoute	Accorde l'autorisation de créer une route associée à un routeur virtuel	Écriture	route*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
CreateVirtualGateway	Accorde l'autorisation de créer une passerelle virtuelle dans un maillage de services	Écriture	virtualGateway*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualNode	Accorde l'autorisation de créer un nœud virtuel dans un maillage de services	Écriture	virtualNode*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateVirtualRouter	Accorde l'autorisation de créer un routeur virtuel dans un maillage de services	Écriture	virtualRouter*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualService	Accorde l'autorisation de créer un service virtuel dans un maillage de services	Écriture	virtualService*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
			virtualRouter		
DeleteGatewayRoute	Accorde l'autorisation de supprimer une route de passerelle existante	Écriture	gatewayRoute*		
DeleteMesh	Accorde l'autorisation de supprimer un maillage de services existant	Écrire	mesh*		
DeleteMeshPolicy [autorisation uniquement]	Accorde l'autorisation de supprimer la politique de contrôle d'accès à la RAM pour un maillage	Écrire	mesh*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRoute	Accorde l'autorisation de supprimer une route existante	Écriture	route*		
DeleteVirtualGateway	Accorde l'autorisation de supprimer une passerelle virtuelle existante	Écriture	virtualGateway*		
DeleteVirtualNode	Accorde l'autorisation de supprimer un nœud virtuel existant	Écriture	virtualNode*		
DeleteVirtualRouter	Accorde l'autorisation de supprimer un routeur virtuel existant	Écriture	virtualRouter*		
DeleteVirtualService	Accorde l'autorisation de supprimer un service virtuel existant	Écriture	virtualService*		
DescribeGatewayRoute	Accorde l'autorisation de décrire une route de passerelle existante	Lecture	gatewayRoute*		
DescribeMesh	Accorde l'autorisation de décrire un maillage de services existant	Lecture	mesh*		
DescribeRoute	Accorde l'autorisation de décrire une route existante	Lecture	route*		
DescribeVirtualGateway	Accorde l'autorisation de décrire une passerelle virtuelle existante	Lecture	virtualGateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeVirtualNode	Accorde l'autorisation de décrire un nœud virtuel existant	Lecture	virtualNode*		
DescribeVirtualRouter	Accorde l'autorisation de décrire un routeur virtuel existant	Lecture	virtualRouter*		
DescribeVirtualService	Accorde l'autorisation de décrire un service virtuel existant	Lecture	virtualService*		
GetMeshPolicy [autorisation uniquement]	Accorde l'autorisation de lire la politique de contrôle d'accès à la RAM pour un maillage	Lecture	mesh*		
ListGatewayRoutes	Accorde l'autorisation de répertorier les routes de passerelle existantes dans un maillage de services	Liste	virtualGateway*		
ListMeshes	Accorde l'autorisation de répertorier les maillages de services existants	Liste			
ListRoutes	Accorde l'autorisation de répertorier les routes existantes dans un maillage de services	Liste	virtualRouter*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource App Mesh	Liste	gatewayRoute		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
ListVirtualGateways	Accorde l'autorisation de répertorier les passerelles virtuelles existantes dans un maillage de services	Liste	mesh*		
ListVirtualNodes	Accorde l'autorisation de répertorier les nœuds virtuels existants	Liste	mesh*		
ListVirtualRouters	Accorde l'autorisation de répertorier les routeurs virtuels existants dans un maillage de services	Liste	mesh*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListVirtualServices	Accorde l'autorisation de répertorier les services virtuels existants dans un maillage de services	List	mesh*		
PutMeshPolicy [autorisation uniquement]	Accorde l'autorisation de définir la politique de contrôle d'accès à la RAM pour un maillage	Écrire	mesh*		
StreamAggregatedResources	Accorde l'autorisation de recevoir des ressources diffusées pour un point de terminaison App Mesh (VirtualNode/VirtualGateway)	Lecture	virtualGateway		
			virtualNode		
TagResource	Accorde l'autorisation de baliser une ressource avec un nom resourceArn spécifié	Identification	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			virtualService		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGatewayRoute	Accorde l'autorisation de mettre à jour une route de passerelle existante pour un maillage de services et une passerelle virtuelle spécifiés	Écriture	gatewayRoute*		
			virtualService		
UpdateMesh	Accorde l'autorisation de mettre à jour un maillage de services existant	Écriture	mesh*		
UpdateRoute	Accorde l'autorisation de mettre à jour une route existante pour un maillage de services et un routeur virtuel spécifiés	Écriture	route*		
			virtualNode		
UpdateVirtualGateway	Accorde l'autorisation de mettre à jour une passerelle virtuelle existante dans un maillage de services spécifié	Écriture	virtualGateway*		
UpdateVirtualNode	Accorde l'autorisation de mettre à jour un nœud virtuel existant dans un maillage de services spécifié	Écriture	virtualNode*		
UpdateVirtualRouter	Accorde l'autorisation de mettre à jour un routeur virtuel existant dans un maillage de services spécifié	Écriture	virtualRouter*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateVirtualService	Accorde l'autorisation de mettre à jour un service virtuel existant dans un maillage de services spécifié	Écrire	virtualService*		
			virtualNode		
			virtualRouter		

Types de ressources définis par AWS App Mesh

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
mesh	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}`	aws:ResourceTag/${TagKey}
virtualService	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	aws:ResourceTag/${TagKey}
virtualNode	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
virtualRouter	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}	aws:ResourceTag/${TagKey}
route	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}	aws:ResourceTag/${TagKey}
virtualGateway	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}	aws:ResourceTag/${TagKey}
gatewayRoute	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS App Mesh

AWS App Mesh définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur de balise dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur de balise attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS App Mesh Preview

AWS App Mesh Preview (préfixe de service :`appmesh-preview`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS App Mesh Preview
- Types de ressources définis par AWS App Mesh Preview
- Clés de condition pour AWS App Mesh Preview

Actions définies par AWS App Mesh Preview

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGatewayRoute	Accorde l'autorisation de créer une route de passerelle associée à une passerelle virtuelle	Écriture	gatewayRoute*		
			virtualService		
CreateMesh	Accorde l'autorisation de créer un maillage de services	Écriture	mesh*		
CreateRoute	Accorde l'autorisation de créer une route associée à un routeur virtuel	Écriture	route*		
			virtualNode		
CreateVirtualGateway	Accorde l'autorisation de créer une passerelle virtuelle dans un maillage de services	Écriture	virtualGateway*		
CreateVirtualNode	Accorde l'autorisation de créer un nœud virtuel dans un maillage de services	Écriture	virtualNode*		
			virtualService		
CreateVirtualRouter	Accorde l'autorisation de créer un routeur virtuel dans un maillage de services	Écriture	virtualRouter*		
CreateVirtualService	Accorde l'autorisation de créer un service virtuel dans un maillage de services	Écriture	virtualService*		
			virtualNode		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			virtualRouter		
DeleteGatewayRoute	Accorde l'autorisation de supprimer une route de passerelle existante	Écriture	gatewayRoute*		
DeleteMesh	Accorde l'autorisation de supprimer un maillage de services existant	Écrire	mesh*		
DeleteMeshPolicy [autorisation uniquement]	Accorde l'autorisation de supprimer la politique de contrôle d'accès à la RAM pour un maillage	Écrire	mesh*		
DeleteRoute	Accorde l'autorisation de supprimer une route existante	Écriture	route*		
DeleteVirtualGateway	Accorde l'autorisation de supprimer une passerelle virtuelle existante	Écriture	virtualGateway*		
DeleteVirtualNode	Accorde l'autorisation de supprimer un nœud virtuel existant	Écriture	virtualNode*		
DeleteVirtualRouter	Accorde l'autorisation de supprimer un routeur virtuel existant	Écriture	virtualRouter*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteVirtualService	Accorde l'autorisation de supprimer un service virtuel existant	Écriture	virtualService*		
DescribeGatewayRoute	Accorde l'autorisation de décrire une route de passerelle existante	Lecture	gatewayRoute*		
DescribeMesh	Accorde l'autorisation de décrire un maillage de services existant	Lecture	mesh*		
DescribeRoute	Accorde l'autorisation de décrire une route existante	Lecture	route*		
DescribeVirtualGateway	Accorde l'autorisation de décrire une passerelle virtuelle existante	Lecture	virtualGateway*		
DescribeVirtualNode	Accorde l'autorisation de décrire un nœud virtuel existant	Lecture	virtualNode*		
DescribeVirtualRouter	Accorde l'autorisation de décrire un routeur virtuel existant	Lecture	virtualRouter*		
DescribeVirtualService	Accorde l'autorisation de décrire un service virtuel existant	Lecture	virtualService*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMeshPolicy [autorisation uniquement]	Accorde l'autorisation de lire la politique de contrôle d'accès à la RAM pour un maillage	Lecture	mesh*		
ListGatewayRoutes	Accorde l'autorisation de répertorier les routes de passerelle existantes dans un maillage de services	Liste	virtualGateway*		
ListMeshes	Accorde l'autorisation de répertorier les maillages de services existants	Liste			
ListRoutes	Accorde l'autorisation de répertorier les routes existantes dans un maillage de services	Liste	virtualRouter*		
ListVirtualGateways	Accorde l'autorisation de répertorier les passerelles virtuelles existantes dans un maillage de services	Liste	mesh*		
ListVirtualNodes	Accorde l'autorisation de répertorier les nœuds virtuels existants	Liste	mesh*		
ListVirtualRouters	Accorde l'autorisation de répertorier les routeurs virtuels existants dans un maillage de services	Liste	mesh*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListVirtualServices	Accorde l'autorisation de répertorier les services virtuels existants dans un maillage de services	List	mesh*		
PutMeshPolicy [autorisation uniquement]	Accorde l'autorisation de définir la politique de contrôle d'accès à la RAM pour un maillage	Écrire	mesh*		
StreamAggregatedResources	Accorde l'autorisation de recevoir des ressources diffusées pour un point de terminaison App Mesh (VirtualNode/VirtualGateway)	Lecture	virtualGateway		
			virtualNode		
UpdateGatewayRoute	Accorde l'autorisation de mettre à jour une route de passerelle existante pour un maillage de services et une passerelle virtuelle spécifiés	Écriture	gatewayRoute*		
			virtualService		
UpdateMesh	Accorde l'autorisation de mettre à jour un maillage de services existant	Écriture	mesh*		
UpdateRoute	Accorde l'autorisation de mettre à jour une route existante pour un maillage de services et un routeur virtuel spécifiés	Écriture	route*		
			virtualNode		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateVirtualGateway	Accorde l'autorisation de mettre à jour une passerelle virtuelle existante dans un maillage de services spécifié	Écriture	virtualGateway*		
UpdateVirtualNode	Accorde l'autorisation de mettre à jour un nœud virtuel existant dans un maillage de services spécifié	Écriture	virtualNode*		
UpdateVirtualRouter	Accorde l'autorisation de mettre à jour un routeur virtuel existant dans un maillage de services spécifié	Écriture	virtualRouter*		
UpdateVirtualService	Accorde l'autorisation de mettre à jour un service virtuel existant dans un maillage de services spécifié	Écrire	virtualService*		
			virtualNode		
			virtualRouter		

Types de ressources définis par AWS App Mesh Preview

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
mesh	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}	
virtualService	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}	
virtualNode	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}	
virtualRouter	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}	
route	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}	
virtualGateway	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}	
gatewayRoute	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}	

Clés de condition pour AWS App Mesh Preview

App Mesh Preview ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte

globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS App Runner

AWS App Runner (préfixe de service :`apprunner`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS App Runner
- Types de ressources définis par AWS App Runner
- Clés de condition pour AWS App Runner

Actions définies par AWS App Runner

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateCustomDomain	Accorde l'autorisation d'associer votre propre nom de domaine à l'URL du sous-	Écrire	service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	domaine AWS App Runner de votre service App Runner				
AssociateWebAcl [autorisation uniquement]	Accorde l'autorisation d'associer le service à une AWS ACL Web WAF	Écrire	service*		
			webacl*		
CreateAutoScalingConfiguration	Autorise la création d'une ressource de configuration de dimensionnement automatique AWS App Runner	Écrire	autoscalingconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Accorde l'autorisation de créer une ressource de connexion AWS App Runner	Écrire	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateObservabilityConfiguration	Autorise la création d'une ressource de configuration d'observabilité AWS App Runner	Écrire	observabilityconfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateService	Accorde l'autorisation de créer une ressource de service AWS App Runner	Écrire	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
CreateVpcConnector	Accorde l'autorisation de créer une ressource de connecteur VPC AWS App Runner	Écrire	vpcconnector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcIngressConnection	Accorde l'autorisation de créer une VpcIngressConnection ressource AWS App Runner	Écrire	vpcingressconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ServiceArn apprunner:VpcId apprunner:VpcEndpointId	
DeleteAutoScalingConfiguration	Autorise la suppression d'une ressource de configuration de dimensionnement automatique AWS App Runner	Écrire	autoscalingconfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConnection	Autorise la suppression d'une ressource de connexion AWS App Runner	Écrire	connection*		
DeleteObservabilityConfiguration	Autorise la suppression d'une ressource de configuration d'observabilité d' AWS App Runner	Écrire	observabilityconfiguration*		
DeleteService	Autorise la suppression d'une ressource de service AWS App Runner	Écrire	service*		
DeleteVpcConnector	Accorde l'autorisation de supprimer une ressource du connecteur VPC AWS App Runner	Écrire	vpcconnector*		
DeleteVpcIngressConnection	Autorise la suppression d'une VpcIngressConnection ressource AWS App Runner	Écrire	vpcingressconnection*		
DescribeAutoScalingConfiguration	Accorde l'autorisation de récupérer la description d'une ressource de configuration de dimensionnement automatique AWS App Runner	Lecture	autoscalingconfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCustomDomains	Accorde l'autorisation de récupérer les descriptions des noms de domaine personnalisés associés à un service AWS App Runner	Lecture	service*		
DescribeObservabilityConfiguration	Accorde l'autorisation de récupérer la description d'une ressource de configuration d'observabilité d' AWS App Runner	Lecture	observabilityconfiguration*		
DescribeOperation	Accorde l'autorisation de récupérer la description d'une opération survenue sur un service AWS App Runner	Lecture	service*		
DescribeService	Accorde l'autorisation de récupérer la description d'une ressource de service AWS App Runner	Lecture	service*		
DescribeVpcConnector	Accorde l'autorisation de récupérer la description d'une ressource du connecteur VPC AWS App Runner	Lecture	vpcconnector*		
DescribeVpcIngressConnection	Accorde l'autorisation de récupérer la description d'une VpcIngressConnection ressource AWS App Runner	Lecture	vpcingressconnection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWebAclForService [autorisation uniquement]	Accorde l'autorisation d'obtenir l'ACL Web AWS WAF associée à un service AWS App Runner	Lecture	service*		
DisassociateCustomDomain	Accorde l'autorisation de dissocier un nom de domaine personnalisé d'un service AWS App Runner	Écrire	service*		
DisassociateWebAcl [autorisation uniquement]	Accorde l'autorisation de dissocier le service d'une ACL AWS Web WAF	Écrire	service*		
ListAssociatedServicesForWebAcl [autorisation uniquement]	Accorde l'autorisation de répertorier les services associés à une AWS ACL Web WAF	List	webacl*		
ListAutoScalingConfigurations	Autorise l'extraction d'une liste des configurations de dimensionnement automatique d' AWS App Runner dans votre Compte AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConnections	Accorde l'autorisation de récupérer une liste des connexions AWS App Runner dans votre Compte AWS	List			
ListObservabilityConfigurations	Accorde l'autorisation de récupérer une liste des configurations d'observabilité d' AWS App Runner dans votre Compte AWS	List			
ListOperations	Accorde l'autorisation de récupérer une liste des opérations survenues sur une ressource de service AWS App Runner	List	service*		
ListServices	Accorde l'autorisation de récupérer une liste des services AWS App Runner en cours d'exécution dans votre Compte AWS	List			
ListServicesForAutoScalingConfiguration	Permet de récupérer la liste des AppRunner services associés à une configuration de dimensionnement automatique d' AWS App Runner dans votre Compte AWS	List	autoscalingconfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les tags associés à une ressource AWS App Runner	Lecture	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
ListVpcConnectors	Permet de récupérer la liste des connecteurs VPC AWS App Runner dans votre Compte AWS	List			
ListVpcIngressConnections	Accorde l'autorisation de récupérer une liste d' AWS App Runner VpcIngressConnections dans votre Compte AWS	List			
PauseService	Accorde l'autorisation de suspendre un service AWS App Runner actif	Écrire	service*		
ResumeService	Autorise la reprise d'un service AWS App Runner actif	Écrire	service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDeployment	Autorise le lancement d'un déploiement manuel vers un service AWS App Runner	Écrire	service*		
TagResource	Accorde l'autorisation d'ajouter des balises ou de mettre à jour les valeurs des balises d'une ressource AWS App Runner	Identification	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource AWS App Runner	Identification	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys	
UpdateDefaultAutoScalingConfiguration	Autorise la mise à jour d'une configuration de dimensionnement automatique d' AWS App Runner pour qu'elle soit la configuration par défaut dans votre Compte AWS	Écrire	autoscalingconfiguration*		
UpdateService	Autorise la mise à jour d'une ressource de service AWS App Runner	Écrire	service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
UpdateVpcIngressConnection	Autorise la mise à jour d'une VpcIngressConnection ressource AWS App Runner	Écrire	vpcingressconnection*		
				apprunner:VpcId apprunner:VpcEndpointId	

Types de ressources définis par AWS App Runner

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
service	`arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}`	aws:ResourceTag/${TagKey}
connection	`arn:${Partition}:apprunner:${Region}:${Account}:connection/${ConnectionName}/${ConnectionId}`	aws:ResourceTag/${TagKey}
autoscalingconfiguration	`arn:${Partition}:apprunner:${Region}:${Account}:autoscalingconfiguration/${AutoscalingConfigurationName}/${AutoscalingConfigurationVersion}/${AutoscalingConfigurationId}`	aws:ResourceTag/${TagKey}
observabilityconfiguration	`arn:${Partition}:apprunner:${Region}:${Account}:observabilityconfiguration/${ObservabilityConfigurationName}/${ObservabilityConfigurationVersion}/${ObservabilityConfigurationId}`	aws:ResourceTag/${TagKey}
vpcconnector	`arn:${Partition}:apprunner:${Region}:${Account}:vpcconnector/${VpcConnectorName}/${VpcConnectorVersion}/${VpcConnectorId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
vpcingressconnection	`arn:${Partition}:apprunner:${Region}:${Account}:vpcingressconnection/${VpcIngressConnectionName}/${VpcIngressConnectionId}`	aws:ResourceTag/${TagKey}
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	

Clés de condition pour AWS App Runner

AWS App Runner définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
apprunner:AutoScalingConfigurationArn	Filtre l'accès par les UpdateService actions CreateService et en fonction de l'ARN d'une AutoScalingConfiguration ressource associée	ARN
apprunner:ConnectionArn	Filtre l'accès par les UpdateService actions CreateService et en fonction de l'ARN d'une ressource de connexion associée	ARN
apprunner:ObservabilityConfigurationArn	Filtre l'accès par les UpdateService actions CreateService et en fonction de l'ARN d'une ObservabilityConfiguration ressource associée	ARN

Clés de condition	Description	Type
apprunner:ServiceArn	Filtre l'accès par CreateVpcIngressConnection action en fonction de l'ARN d'une ressource de service associée	ARN
apprunner:VpcConnectorArn	Filtre l'accès par les UpdateService actions CreateService et en fonction de l'ARN d'une VpcConnector ressource associée	ARN
apprunner:VpcEndpointId	Filtre l'accès par les UpdateVpcIngressConnection actions CreateVpcIngressConnection et en fonction du point de terminaison VPC indiqué dans la demande	String
apprunner:VpcId	Filtre l'accès par les UpdateVpcIngressConnection actions CreateVpcIngressConnection et en fonction du VPC contenu dans la demande	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des actions basées sur la présence de paires clé-valeur d'identification dans la requête	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des actions basées sur les paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des actions basées sur la présence de clés d'identification dans la requête	ArrayOfString

Actions, ressources et clés de condition pour AWS App Studio

AWS App Studio (préfixe de service :`appstudio`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS App Studio
- Types de ressources définis par AWS App Studio
- Clés de condition pour AWS App Studio

Actions définies par AWS App Studio

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountStatus [autorisation uniquement]	Accorde l'autorisation de décrire le statut actuel du compte	Lecture			
GetEnablementJobStatus [autorisation uniquement]	Accorde l'autorisation de récupérer le statut d'une tâche d'activation	Lecture			
StartEnablementJob [autorisation uniquement]	Donne l'autorisation de soumettre une offre d'habilitation	Écrire			
StartRollbackEnabl	Autorise l'annulation d'une tâche d'habilitation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ementJob [autorisation uniquement]					
StartTeam Deployment [autorisation uniquement]	Accorde l'autorisation de démarrer un déploiement d'équipe	Écrire			

Types de ressources définis par AWS App Studio

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
instance	`arn:${Partition}:appstudio:${Region}:${Account}:instance/${InstanceId}`	
application	`arn:${Partition}:appstudio:${Region}:${Account}:application/${ApplicationId}`	
connector	`arn:${Partition}:appstudio:${Region}:${Account}:connector/${ConnectionId}`	

Clés de condition pour AWS App Studio

App Studio ne possède aucune clé de contexte spécifique à un service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS App2Container

AWS App2Container (préfixe de service :`a2c`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS App2Container
- Types de ressources définis par AWS App2Container
- Clés de condition pour AWS App2Container

Actions définies par AWS App2Container

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les

ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContainerizationJobDetails	Accorde l'autorisation d'obtenir les détails de toutes les tâches de conteneurisation	Lecture			
GetDeploymentJobDetails	Accorde l'autorisation d'obtenir les détails de toutes les tâches de déploiement	Lecture			
StartContainerizationJob	Accorde l'autorisation de démarrer une tâche de conteneurisation	Écrire			
StartDeploymentJob	Accorde l'autorisation de démarrer une tâche déploiement	Écrire			

Types de ressources définis par AWS App2Container

AWS App2Container ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS App2Container, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS App2Container

App2Container ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS AppConfig

AWS AppConfig (préfixe de service :`appconfig`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS AppConfig
- Types de ressources définis par AWS AppConfig
- Clés de condition pour AWS AppConfig

Actions définies par AWS AppConfig

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApplication	Accorde l'autorisation de créer une application	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfigurationProfile	Accorde l'autorisation de créer un profil de configuration	Écriture	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeploymentStrategy	Accorde l'autorisation de créer une stratégie de déploiement	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Accorde l'autorisation de créer un environnement	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtension	Accorde l'autorisation de créer une extension	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExtensionAssociation	Accorde l'autorisation de créer une association d'extension	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHostedConfigurationVersion	Accorde l'autorisation de créer une version de configuration hébergée	Écriture	application*		
			configurationprofile*		
DeleteApplication	Accorde l'autorisation de supprimer une application	Écriture	application*		
DeleteConfigurationProfile	Accorde l'autorisation de supprimer un profil de configuration	Écriture	application*		
			configurationprofile*		
DeleteDeploymentStrategy	Accorde l'autorisation de supprimer une stratégie de déploiement	Écriture	deploymentstrategy*		
DeleteEnvironment	Accorde l'autorisation de supprimer un environnement	Écrire	application*		
			environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteExtension	Accorde l'autorisation de supprimer une extension	Écrire	extension*		
DeleteExtensionAssociation	Accorde l'autorisation de supprimer une association d'extension	Écrire	extensionassociation*		
DeleteHostedConfigurationVersion	Accorde l'autorisation de supprimer une version de configuration hébergée	Écrire	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetAccountSettings	Accorde l'autorisation de consulter les paramètres de l'ensemble du compte AppConfig	Lecture			
GetApplication	Accorde l'autorisation d'afficher les détails d'une application	Lecture	application*		
				aws:ResourceTag/${TagKey}	
GetConfiguration	Accorde l'autorisation d'afficher les détails d'une configuration	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			configurationprofile*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetConfigurationProfile	Accorde l'autorisation d'afficher les détails d'un profil de configuration	Lecture	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
GetDeployment	Accorde l'autorisation d'afficher les détails d'un déploiement	Lecture	application*		
			deployment*		
			environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetDeploymentStrategy	Accorde l'autorisation d'afficher les détails d'une stratégie de déploiement	Lecture	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	Accorde l'autorisation d'afficher les détails d'un environnement	Lecture	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetExtension	Accorde l'autorisation de consulter les détails d'une extension	Lecture	extension*		
				aws:ResourceTag/${TagKey}	
GetExtensionAssociation	Accorde l'autorisation de consulter les détails d'une association d'extension	Lecture	extensionassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetHostedConfigurationVersion	Accorde l'autorisation d'afficher les détails d'une version de configuration hébergée	Lecture	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetLatestConfiguration	Accorde l'autorisation de récupérer une configuration déployée	Lecture	configuration*		
				aws:ResourceTag/${TagKey}	
ListApplications	Accorde l'autorisation de répertorier les applications de votre compte	Liste			
ListConfigurationProfiles	Accorde l'autorisation de répertorier les profils de configuration d'une application	Liste	application*		
ListDeploymentStrategies	Accorde l'autorisation de répertorier les stratégies de déploiement de votre compte	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDeployments	Accorde l'autorisation de répertorier les déploiements d'un environnement	Liste	application*		
			environment*		
ListEnvironments	Accorde l'autorisation de répertorier les environnements d'une application	List	application*		
ListExtensionAssociations	Accorde l'autorisation de répertorier les associations d'extension de votre compte	List			
ListExtensions	Accorde l'autorisation de répertorier les extensions de votre compte	List			
ListHostedConfigurationVersions	Accorde l'autorisation de répertorier les versions de configuration hébergées pour un profil de configuration	Liste	application*		
			configurationprofile*		
ListTagsForResource	Accorde l'autorisation d'afficher une liste de identifications de ressource pour une ressource spécifiée	Lecture	application		
			configurationprofile		
			deployment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:ResourceTag/${TagKey}	
StartConfigurationSession	Accorde l'autorisation de démarrer une session de configuration	Écrire	configuration*		
				aws:ResourceTag/${TagKey}	
StartDeployment	Accorde l'autorisation de lancer un déploiement	Écriture	application*		
			configurationprofile*		
			deploymentstrategy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopDeployment	Accorde l'autorisation d'arrêter un déploiement	Écrire	application*		
			deployment*		
			environment*		
TagResource	Accorde l'autorisation de baliser une ressource appconfig	Identification	application		
			configuration		
			configurationprofile		
			deployment		
			deploymentstrategy		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			environment		
			extension		
			extensionassociation		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource appconfig	Identification	application		
			configuration		
			configurationprofile		
			deployment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys	
UpdateAccountSettings	Accorde l'autorisation de modifier les paramètres de l'ensemble du compte AppConfig	Écrire			
UpdateApplication	Accorde l'autorisation de modifier une application	Écriture	application*		
				aws:ResourceTag/${TagKey}	
UpdateConfigurationProfile	Accorde l'autorisation de modifier un profil de configuration	Écriture	application*		
			configurationprofile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateDeploymentStrategy	Accorde l'autorisation de modifier une stratégie de déploiement	Écriture	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	Accorde l'autorisation de modifier un environnement	Écrire	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
UpdateExtension	Accorde l'autorisation de modifier une extension	Écrire	extension*		
				aws:ResourceTag/${TagKey}	
UpdateExtensionAssociation	Accorde l'autorisation de modifier une association d'extension	Écrire	extensionassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ValidateConfiguration	Accorde l'autorisation de valider une configuration	Écrire	application*		
			configurationprofile*		

Types de ressources définis par AWS AppConfig

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
environment	`arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
configurationprofile	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}
deploymentstrategy	arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/deployment/${DeploymentNumber}	aws:ResourceTag/${TagKey}
hostedconfigurationversion	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}	
configuration	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/configuration/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}
extension	arn:${Partition}:appconfig:${Region}:${Account}:extension/${ExtensionId}/${ExtensionVersionNumber}	aws:ResourceTag/${TagKey}
extensionassociation	arn:${Partition}:appconfig:${Region}:${Account}:extensionassociation/${ExtensionAssociationId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS AppConfig

AWS AppConfig définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées spécifié pour une balise spécifiée	String
aws:ResourceTag/${TagKey}	Filtre l'accès par une paire clé-valeur de balise attribuée à la ressource AWS	String
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS AppFabric

AWS AppFabric (préfixe de service :`appfabric`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS AppFabric
- Types de ressources définis par AWS AppFabric
- Clés de condition pour AWS AppFabric

Actions définies par AWS AppFabric

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetUserAccessTasks	Accorde l'autorisation de lancer des tâches d'accès utilisateur pour plusieurs utilisateurs	Écrire	appbundle*		
ConnectAppAuthorization	Octroie l'autorisation de connecter les autorisations d'application.	Écrire	appauthorization*		
			appbundle*		
CreateAppAuthorization	Octroie l'autorisation de créer des autorisations d'application pour les groupes d'applications.	Écrire	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBundle	Octroie l'autorisation de créer des groupes d'applications sur votre compte.	Écrire		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateIngestion	Octroie l'autorisation de créer des ingestions pour les groupes d'applications.	Écrire	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestionDestination	Octroie l'autorisation de créer des destinations d'ingestion pour les groupes d'applications.	Écrire	appbundle*		
			ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppAuthorization	Octroie l'autorisation de supprimer les autorisations d'application au sein d'un groupe d'applications.	Écrire	appauthorization*		
			appbundle*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAppBundle	Octroie l'autorisation de supprimer des groupes d'applications de votre compte.	Écrire	appbundle*		
DeleteIngestion	Octroie l'autorisation de supprimer des ingestions au sein d'un groupe d'applications.	Écrire	appbundle*		
			ingestion*		
DeleteIngestionDestination	Accorde l'autorisation de supprimer des destinations au sein d'une ingestion	Écrire	appbundle*		
			ingestion*		
			ingestiondestination*		
GetAppAuthorization	Octroie l'autorisation de consulter les détails des autorisations d'application.	Lecture	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAppBundle	Octroie l'autorisation de consulter les détails des groupes d'applications.	Lecture	appbundle*		
				aws:ResourceTag/${TagKey}	
GetIngestion	Accorde l'autorisation de consulter les détails des ingestions	Lecture	appbundle*		
			ingestion*		
				aws:ResourceTag/${TagKey}	
GetIngestionDestination	Accorde l'autorisation de consulter les détails des destinations d'ingestion	Lecture	appbundle*		
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAppAuthorizations	Octroie l'autorisation de récupérer une liste d'autorisations d'application au sein d'un groupe d'applications.	List	appbundle*		
ListAppBundles	Octroie l'autorisation de récupérer une liste de groupes d'applications de votre compte.	List			
ListIngestionDestinations	Accorde l'autorisation de récupérer une liste de destinations au sein d'une ingestion	List	appbundle*		
			ingestion*		
ListIngestions	Octroie l'autorisation de récupérer une liste d'ingestions au sein d'un groupe d'applications.	List	appbundle*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour les AppFabric ressources	Lecture	appauthorization		
			appbundle		
			ingestion		
			ingestion destination		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartIngestion	Accorde l'autorisation de lancer des ingestions	Écrire	appbundle*		
			ingestion*		
StartUserAccessTasks	Accorde l'autorisation de lancer des tâches d'accès utilisateur	Écrire	appbundle*		
StopIngestion	Accorde l'autorisation d'arrêter les ingestions	Écrire	appbundle*		
			ingestion*		
TagResource	Accorde l'autorisation de baliser AppFabric les ressources	Identification	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer le balisage des ressources AppFabric	Identification	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
				aws:TagKeys	
UpdateAppAuthorization	Octroie l'autorisation de mettre à jour les autorisations d'application au sein des groupes d'applications.	Écrire	appauthorization*		
			appbundle*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateIngestionDestination	Accorde l'autorisation de mettre à jour les destinations au sein des ingestions	Écrire	appbundle*		
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS AppFabric

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
appbundle	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppBundleIdentifier}`	aws:ResourceTag/${TagKey}
appauthorization	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/appauthorization/${AppAuthorizationIdentifier}`	aws:ResourceTag/${TagKey}
ingestion	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}`	aws:ResourceTag/${TagKey}
ingestion destination	`arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}/ingestiondestination/${IngestionDestinationIdentifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS AppFabric

AWS AppFabric définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon AppFlow

Amazon AppFlow (préfixe de service :`appflow`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon AppFlow
- Types de ressources définis par Amazon AppFlow
- Clés de condition pour Amazon AppFlow

Actions définies par Amazon AppFlow

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelFlowExecutions	Autorise l'annulation des exécutions en cours d'un flux Amazon AppFlow	Écrire	flow*		
CreateConnectorProfile	Accorde l'autorisation de créer un profil de connexion à utiliser avec Amazon AppFlow Flows	Écrire			
CreateFlow	Accorde l'autorisation de créer un AppFlow flux Amazon	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConnectorProfile	Accorde l'autorisation de supprimer un profil de connexion configuré sur Amazon AppFlow	Écrire	connectorprofile*		
DeleteFlow	Accorde l'autorisation de supprimer un AppFlow flux Amazon	Écrire	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeConnector	Accorde l'autorisation de décrire un connecteur	Lecture	connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	enregistré sur Amazon AppFlow				
DescribeConnectorEntity	Accorde l'autorisation de décrire tous les champs d'un objet dans un profil de connexion configuré dans Amazon AppFlow	Lecture	connectorprofile*		
DescribeConnectorFields [autorisation uniquement]	Accorde l'autorisation de décrire tous les champs d'un objet dans un profil de connexion configuré dans Amazon AppFlow (console uniquement)	Lecture	connectorprofile*		
DescribeConnectorProfiles	Accorde l'autorisation de décrire tous les profils de connexion configurés dans Amazon AppFlow	Lecture			
DescribeConnectors	Autorise à décrire tous les connecteurs pris en charge par Amazon AppFlow	Lecture			
DescribeFlow	Accorde l'autorisation de décrire un flux spécifique configuré dans Amazon AppFlow	Lecture	flow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFlowExecution [autorisation uniquement]	Accorde l'autorisation de décrire toutes les exécutions de flux pour un flux configuré dans Amazon AppFlow (console uniquement)	Lecture	flow*		
DescribeFlowExecutionRecords	Accorde l'autorisation de décrire toutes les exécutions de flux pour un flux configuré dans Amazon AppFlow	Lecture	flow*		
DescribeFlows [autorisation uniquement]	Accorde l'autorisation de décrire tous les flux configurés dans Amazon AppFlow (console uniquement)	Lecture			
ListConnectorEntities	Accorde l'autorisation de répertorier tous les objets d'un profil de connexion configuré dans Amazon AppFlow	List	connectorprofile*		
ListConnectorFields [autorisation uniquement]	Accorde l'autorisation de répertorier tous les objets d'un profil de connexion configuré dans Amazon AppFlow (console uniquement)	Lecture	connectorprofile*		
ListConnectors	Accorde l'autorisation de répertorier tous les connecteurs pris en charge sur Amazon AppFlow	List	connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFlows	Accorde l'autorisation de répertorier tous les flux configurés dans Amazon AppFlow	List	flow*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour un flux.	Lecture	flow*		
RegisterConnector	Accorde l'autorisation d'enregistrer un AppFlow connecteur Amazon	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
ResetConnectorMetadataCache	Autorise la réinitialisation des métadonnées des entités de connecteur AppFlow stockées par Amazon dans son cache	Écrire	connectorprofile*		
RunFlow [autorisation uniquement]	Accorde l'autorisation d'exécuter un flux configuré dans Amazon AppFlow (console uniquement)	Écrire	flow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartFlow	Accorde l'autorisation d'activer (pour les flux planifiés et déclenchés par des événements) ou d'exécuter (pour les flux à la demande) un flux configuré dans Amazon AppFlow	Écrire	flow*		
StopFlow	Accorde l'autorisation de désactiver un flux planifié ou déclenché par un événement configuré dans Amazon AppFlow	Écrire	flow*		
TagResource	Accorde l'autorisation de baliser un flux ou un connecteur	Identification	connector		
			flow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UnRegisterConnector	Accorde l'autorisation de désinscrire un connecteur sur Amazon AppFlow	Écrire	connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'un flux ou d'un connecteur	Identification	connector		
			flow		
				aws:TagKeys	
UpdateConnectorProfile	Accorde l'autorisation de mettre à jour un profil de connexion configuré dans Amazon AppFlow	Écrire	connectorprofile*		
UpdateConnectorRegistration	Accorde l'autorisation de mettre à jour un connecteur enregistré configuré dans Amazon AppFlow	Écrire	connector*		
UpdateFlow	Accorde l'autorisation de mettre à jour un flux configuré dans Amazon AppFlow	Écrire	flow*		
UseConnectorProfile [autorisation uniquement]	Accorde l'autorisation d'utiliser un profil de connecteur lors de la création d'un flux dans Amazon AppFlow	Écrire	connectorprofile*		

Types de ressources définis par Amazon AppFlow

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
connector profile	`arn:${Partition}:appflow:${Region}:${Account}:connectorprofile/${ProfileName}`	
flow	`arn:${Partition}:appflow:${Region}:${Account}:flow/${FlowName}`	aws:ResourceTag/${TagKey}
connector	`arn:${Partition}:appflow:${Region}:${Account}:connector/${ConnectorLabel}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon AppFlow

Amazon AppFlow définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des étiquettes	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence d'étiquettes obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon AppIntegrations

Amazon AppIntegrations (préfixe de service :`app-integrations`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon AppIntegrations
- Types de ressources définis par Amazon AppIntegrations
- Clés de condition pour Amazon AppIntegrations

Actions définies par Amazon AppIntegrations

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApplication	Accorde l'autorisation de créer une application.	Écrire	application*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssociation [autorisation uniquement]	Accorde l'autorisation de créer un ApplicationAssociation	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegration	Accorde l'autorisation de créer un nouveau DataIntegration	Écrire	data-integration*		appflow:DeleteFlow appflow:DescribeCo

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					nnectorProfiles iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant profile:GetDomain profile:GetProfileObjectType s3:GetBucketNotification s3:GetEncryptionConfiguration

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					s3:PutBucketNotification
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataIntegrationAssociation	Accorde l'autorisation de créer un DataIntegrationAssociation	Écrire	data-integration*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:TagResource appflow:UseConnectorProfile profile:CreateSnapshot profile:GetSnapshot

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegrationSchedule	Accorde l'autorisation de créer un calendrier d'intégration des données	Écrire	data-integration*		
CreateEventIntegration	Accorde l'autorisation de créer un nouveau EventIntegration	Écrire	event-integration*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEventIntegrationAssociation [autorisation uniquement]	Accorde l'autorisation de créer un EventIntegrationAssociation	Écrire	event-integration*		events:PutRule events:PutTargets
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	application*		
				aws:ResourceTag/${TagKey}	
DeleteApplicationAssociation [autorisation uniquement]	Accorde l'autorisation de supprimer un ApplicationAssociation	Écrire	application-association*		
DeleteDataIntegration	Accorde l'autorisation de supprimer un DataIntegration	Écrire	data-integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDataIntegrationAssociation [autorisation uniquement]	Accorde l'autorisation de supprimer un DataIntegrationAssociation	Écrire	data-integration-association*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:StopFlow appflow:TagResource appflow:UseConnectorProfile
DeleteEventIntegration	Accorde l'autorisation de supprimer un EventIntegration	Écrire	event-integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEventIntegrationAssociation [autorisation uniquement]	Accorde l'autorisation de supprimer un EventIntegrationAssociation	Écrire	event-integration-association*		events:DeleteRule events:ListTargetsByRule events:RemoveTargets
GetApplication	Accorde l'autorisation d'afficher les détails d'une application.	Lecture	application*		
				aws:ResourceTag/${TagKey}	
GetDataIntegration	Accorde l'autorisation de consulter les détails sur DataIntegrations	Lecture	data-integration*		
				aws:ResourceTag/${TagKey}	
GetDataIntegrationExecution	Accorde l'autorisation d'obtenir des détails sur l'exécution d'une intégration de données	Lecture	data-integration*		
GetDataIntegrationSchedule	Accorde l'autorisation d'obtenir des informations sur un calendrier d'intégration de données	Lecture	data-integration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEventIntegration	Accorde l'autorisation de consulter les détails sur EventIntegrations	Lecture	event-integration*		
				aws:ResourceTag/${TagKey}	
ListApplicationAssociations	Accorde l'autorisation de mettre en vente ApplicationAssociations	List			
ListApplications	Accorde l'autorisation de répertorier les applications.	List			
ListDataIntegrationAssociations	Accorde l'autorisation de mettre en vente DataIntegrationAssociations	List			
ListDataIntegrationExecutions	Accorde l'autorisation de répertorier les exécutions d'intégration de données	List	data-integration*		
ListDataIntegrationSchedules	Accorde l'autorisation de répertorier les calendriers d'intégration des données	List	data-integration*		
ListDataIntegrations	Accorde l'autorisation de mettre en vente DataIntegrations	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEventIntegrationAssociations	Accorde l'autorisation de mettre en vente EventIntegrationAssociations	Lecture			
ListEventIntegrations	Accorde l'autorisation de mettre en vente EventIntegrations	List			
ListTagsForResource	Accorde l'autorisation de créer des balises pour une AppIntegration ressource Amazon	Lecture	application		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDataIntegrationExecution	Autorise le lancement d'une exécution d'intégration de données	Écrire	data-integration*		profile:CreateSegmentSnapshot profile:CreateSnapshot
TagResource	Accorde l'autorisation de baliser une AppIntegration ressource Amazon	Identification	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource Amazon AppIntegration	Identification	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApplication	Accorde l'autorisation de modifier une application.	Écrire	application*		
				aws:ResourceTag/${TagKey}	
UpdateDataIntegration	Accorde l'autorisation de modifier un DataIntegration	Écrire	data-integration*		
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationAssociation	Accorde l'autorisation de modifier un DataIntegrationAssociation	Écrire	data-integration-association*		profile:CreateSnapshot profile:GetSnapshot
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataIntegrationSchedule	Autorise la mise à jour d'un calendrier d'intégration des données	Écrire	data-integration*		
UpdateEventIntegration	Accorde l'autorisation de modifier un EventIntegration	Écrire	event-integration*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon AppIntegrations

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
event-integration	`arn:${Partition}:app-integrations:${Region}:${Account}:event-integration/${EventIntegrationName}`	aws:ResourceTag/${TagKey}
event-integration-association	`arn:${Partition}:app-integrations:${Region}:${Account}:event-integration-association/${EventIntegrationName}/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
data-integration	arn:${Partition}:app-integrations:${Region}:${Account}:data-integration/${DataIntegrationId}	aws:ResourceTag/${TagKey}
data-integration-association	arn:${Partition}:app-integrations:${Region}:${Account}:data-integration-association/${DataIntegrationId}/${ResourceId}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:app-integrations:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
application-association	arn:${Partition}:app-integrations:${Region}:${Account}:application-association/${ApplicationId}/${ApplicationAssociationId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon AppIntegrations

Amazon AppIntegrations définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Application Auto Scaling

AWS Application Auto Scaling (préfixe de service :`application-autoscaling`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Application Auto Scaling
- Types de ressources définis par AWS Application Auto Scaling
- Clés de condition pour AWS Application Auto Scaling

Actions définies par AWS Application Auto Scaling

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteScalingPolicy	Accorde l'autorisation de supprimer une politique de mise à l'échelle	Écrire	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeleteScheduledAction	Accorde l'autorisation de supprimer une action planifiée	Écrire	ScalableTarget*		
				application-autoscaling:service-namespace application-autosc	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aling:scalable-dimension	
DeregisterScalableTarget	Accorde l'autorisation d'annuler l'enregistrement d'une cible évolutive	Écrire	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DescribeScalableTargets	Accorde l'autorisation de décrire une ou plusieurs cibles évolutives dans l'espace de noms spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeScalingActivities	Accorde l'autorisation de décrire un ensemble d'activités de mise à l'échelle ou toutes les activités de mise à l'échelle dans l'espace de noms spécifié	Lecture			
DescribeScalingPolicies	Accorde l'autorisation de décrire un ensemble de politiques de mise à l'échelle ou toutes les politiques de mise à l'échelle dans l'espace de noms spécifié	Lecture			
DescribeScheduledActions	Accorde l'autorisation de décrire un ensemble d'actions planifiées ou toutes les actions planifiées dans l'espace de noms spécifié	Lecture			
GetPredictiveScalingForecast	Accorde l'autorisation de récupérer les données de prévision pour une politique de mise à l'échelle prédictive	List			
ListTagsForResource	Octroie l'autorisation de répertorier les balises pour une cible évolutive	Lecture	ScalableTarget*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutScalingPolicy	Accorde l'autorisation de créer et de mettre à jour une politique de mise à l'échelle pour une cible évolutive	Écrire	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
PutScheduledAction	Accorde l'autorisation de créer et de mettre à jour une action planifiée pour une cible évolutive	Écrire	ScalableTarget*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterScalableTarget	Accorde l'autorisation d'enregistrer AWS ou de personnaliser des ressources en tant que cibles évolutives avec Application Auto Scaling et de mettre à jour les paramètres de configuration utilisés pour gérer une cible évolutive	Écrire	ScalableTarget*		application-autoscaling:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
TagResource	Octroie l'autorisation de baliser une cible évolutive	Identification	ScalableTarget*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Octroie l'autorisation de retirer les balises d'une cible évolutive	Identification	ScalableTarget*		
				aws:TagKeys	

Types de ressources définis par AWS Application Auto Scaling

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
ScalableTarget	`arn:${Partition}:application-autoscaling:${Region}:${Account}:scalable-target/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Application Auto Scaling

AWS Application Auto Scaling définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
application-autoscaling:scalable-dimension	Filtre l'accès en fonction de la dimension évolutive transmise dans la demande	String
application-autoscaling:service-namespace	Filtre l'accès en fonction de l'espace de noms du service transmis dans la demande	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Application Discovery Arsenal

Application Discovery Arsenal (préfixe de service : `arsenal`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Application Discovery Arsenal
- Types de ressources définis par Application Discovery Arsenal
- Clés de condition pour Application Discovery Arsenal

Actions définies par Application Discovery Arsenal

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterOnPremisesAgent [autorisation uniquement]	Autorise l'enregistrement des collecteurs de données AWS fournis auprès de l'Application Discovery Service	Écrire			

Types de ressources définis par Application Discovery Arsenal

Application Discovery Arsenal ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à Application Discovery Arsenal, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Application Discovery Arsenal

Application Discovery Arsenal ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Application Discovery Service

AWS Application Discovery Service (préfixe de service :`discovery`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Application Discovery Service
- Types de ressources définis par AWS Application Discovery Service
- Clés de condition pour AWS Application Discovery Service

Actions définies par AWS Application Discovery Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateConfigurationItemsToApplication	Accorde l'autorisation à AssociateConfigurationItemsToApplication l'API. AssociateConfigurationItemsToApplication associe un ou plusieurs éléments de configuration à une application	Écrire			
BatchDeleteAgents	Accorde l'autorisation à BatchDeleteAgents l'API. BatchDeleteAgents supprime un ou plusieurs agents/data agents de recouvrement associés à votre compte, chacun étant identifié par son identifiant d'agent. La suppression d'un collecteur de données ne supprime pas les données collectées précédemment.	Écrire			
BatchDeleteImportData	Accorde l'autorisation à BatchDeleteImportData l'API. BatchDeleteImportData supprime une ou plusieurs tâches d'importation de Migration Hub, chacune étant identifiée par son ID d'importation. Chaque tâche d'importation comporte un certain nombre d'enregistrements, qui	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	peuvent identifier des serveurs ou des applications				
CreateApplication	Accorde l'autorisation à CreateApplication l'API. CreateApplication crée une application avec le nom et la description donnés	Écrire			
CreateTags	Accorde l'autorisation à CreateTags l'API. CreateTags crée une ou plusieurs balises pour les éléments de configuration. Les balises sont des métadonnées vous permettant de classer les ressources informatiques. Cette API accepte une liste de plusieurs éléments de configuration	Identification			
DeleteApplications	Accorde l'autorisation à DeleteApplications l'API. DeleteApplications supprime une liste d'applications et leurs associations avec des éléments de configuration	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTags	Accorde l'autorisation à DeleteTags l'API. DeleteTags supprime l'association entre les éléments de configuration et une ou plusieurs balises. Cette API accepte une liste de plusieurs éléments de configuration	Identification		aws:TagKeys	
DescribeAgents	Accorde l'autorisation à DescribeAgents l'API. DescribeAgents répertorie les agents ou le connecteur par ID ou répertorie tous les agents agents/Connectors associés à votre utilisateur si vous n'avez pas spécifié d'identifiant	Lecture			
DescribeBatchDeleteConfigurationTask	Accorde l'autorisation à DescribeBatchDeleteConfigurationTask l'API. DescribeBatchDeleteConfigurationTask renvoie les attributs relatifs à une tâche de suppression par lots visant à supprimer un ensemble d'éléments de configuration. L'ID de tâche fourni doit être l'ID de tâche reçu à partir de la sortie de StartBatchDeleteConfigurationTask	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeConfigurations	Accorde l'autorisation à DescribeConfigurations l'API. DescribeConfigurations récupère les attributs d'une liste d'éléments IDs de configuration. Tous les éléments fournis IDs doivent concerner le même type de ressource (serveur, application, processus ou connexion). Les champs de sortie sont spécifiques au type de ressource sélectionné. Par exemple, la sortie d'un élément de configuration de serveur inclut une liste d'attributs relatifs au serveur, tels que le nom d'hôte, le système d'exploitation et le nombre de cartes réseau	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeContinuousExports	Accorde l'autorisation à DescribeContinuousExports l'API. DescribeContinuousExports répertorie les exportations telles que spécifiées par ID. Toutes les exportations continues associées à votre utilisateur peuvent être répertoriées si vous appelez DescribeContinuousExports telles quelles sans passer de paramètres	Lecture			
DescribeExportConfigurations	Accorde l'autorisation à DescribeExportConfigurations l'API. DescribeExportConfigurations récupère le statut d'un processus d'exportation donné. Vous pouvez récupérer le statut de 100 processus au maximum	Lecture			
DescribeExportTasks	Accorde l'autorisation à DescribeExportTasks l'API. DescribeExportTasks récupérer le statut d'une ou de plusieurs tâches d'exportation. Vous pouvez récupérer le statut de 100 tâches d'exportation au maximum	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeImportTasks	Accorde l'autorisation à DescribeImportTasks l'API. DescribeImportTasks renvoie un ensemble de tâches d'importation pour votre utilisateur, y compris les informations de statut, les heures IDs, l'URL de l'objet Amazon S3 pour le fichier d'importation, etc.	List			
DescribeTags	Accorde l'autorisation à DescribeTags l'API. DescribeTags récupère une liste d'éléments de configuration marqués d'une balise spécifique. Ou récupère une liste de toutes les identifications attribuées à un élément de configuration spécifique	Lecture			
DisassociateConfigurationItemsFromApplication	Accorde l'autorisation à DisassociateConfigurationItemsFromApplication l'API. DisassociateConfigurationItemsFromApplication dissocie un ou plusieurs éléments de configuration d'une application	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportConfigurations	Accorde l'autorisation à ExportConfigurations l'API. ExportConfigurations exporte toutes les données de configuration découvertes vers un compartiment Amazon S3 ou une application qui vous permet de visualiser et d'évaluer les données. Les données comprennent les identifications et les associations d'identifications, les processus, les connexions, les serveurs et les performances du système	Écrire			
GetDiscoverySummary	Accorde l'autorisation à GetDiscoverySummary l'API. GetDiscoverySummary récupère un bref résumé des actifs découverts	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetNetworkConnectionGraph	Accorde l'autorisation à GetNetworkConnectionGraph l'API. GetNetworkConnectionGraph accepte la liste d'entrée de l'une des adresses IP, des identifiants de serveur ou des identifiants de nœuds. Renvoie une liste de nœuds et de périphéries qui aident le client à visualiser le graphique de connexion réseau. Cette API est utilisée pour visualiser les fonctionnalités du graphe de réseau dans MigrationHub la console	Lecture			
ListConfigurations	Accorde l'autorisation à ListConfigurations l'API. ListConfigurations récupère une liste d'éléments de configuration en fonction des critères que vous spécifiez dans un filtre. Les critères de filtrage identifient les exigences en matière de relation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServerNeighbors	Accorde l'autorisation à ListServerNeighbors l'API. ListServerNeighbors récupère une liste de serveurs situés à un saut réseau d'un serveur spécifié	List			
StartBatchDeleteConfigurationTask	Accorde l'autorisation à StartBatchDeleteConfigurationTask l'API. StartBatchDeleteConfigurationTask lance une suppression par lots asynchrone de vos éléments de configuration. Tous les éléments fournis IDs doivent concerner le même type de ressource (serveur, application, processus ou connexion). La sortie est un ID de tâche unique que vous pouvez utiliser pour vérifier la progression des suppressions.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartContinuousExport	Accorde l'autorisation à StartContinuousExport l'API. StartContinuousExport démarrer le flux continu des données découvertes par l'agent vers Amazon Athena	Écrire			iam:AttachRolePolicy iam:CreatePolicy iam:CreateRole iam:CreateServiceLinkedRole
StartDataCollectionByAgentIds	Accorde l'autorisation à StartDataCollectionByAgentIds l'API. StartDataCollectionByAgentIds indique aux agents ou connecteurs spécifiés de commencer à collecter des données	Écrire			
StartExportTask	Accorde l'autorisation à StartExportTask l'API. StartExportTask exporter les données de configuration relatives aux éléments de configuration et aux relations découverts vers un compartiment S3 dans un format spécifié	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartImportTask	Accorde l'autorisation à StartImportTask l'API. StartImportTask lance une tâche d'importation. La fonctionnalité d'importation de Migration Hub vous permet d'importer les détails de votre environnement sur site directement AWS sans avoir à utiliser les outils Application Discovery Service (ADS) tels que le Discovery Connector ou le Discovery Agent. Vous avez ainsi la possibilité d'effectuer des évaluations de migrations et des planifications directement à partir de vos données importées, y compris la possibilité de regrouper vos appareils en tant qu'applications et de suivre leur statut de migration	Écrire			discovery:AssociateConfigurationItemsToApplication discovery:CreateApplication discovery:CreateTags discovery:GetDiscoverySummary discovery:ListConfigurations s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopContinuousExport	Accorde l'autorisation à StopContinuousExport l'API. StopContinuousExport arrête le flux continu de données découvertes par l'agent vers Amazon Athena	Écrire			
StopDataCollectionByAgentIds	Accorde l'autorisation à StopDataCollectionByAgentIds l'API. StopDataCollectionByAgentIds demande aux agents ou connecteurs spécifiés d'arrêter de collecter des données	Écrire			
UpdateApplication	Accorde l'autorisation à UpdateApplication l'API. UpdateApplication met à jour les métadonnées d'une application	Écrire			

Types de ressources définis par AWS Application Discovery Service

AWS Application Discovery Service ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Application Discovery Service, spécifiez `"Resource": "*"` dans votre politique.

> **Note**
>
> Pour séparer les accès, créez et utilisez AWS des comptes distincts.

Clés de condition pour AWS Application Discovery Service

AWS Application Discovery Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le service de migration AWS d'applications

AWS Le service de migration d'applications (préfixe de service :`mgn`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service de migration des AWS applications
- Types de ressources définis par le service de migration des AWS applications
- Clés de condition pour le service de migration d' AWS applications

Actions définies par le service de migration des AWS applications

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ArchiveApplication	Accorde l'autorisation d'archiver une application	Écrire	ApplicationResource*		
ArchiveWave	Accorde l'autorisation d'archiver une vague	Écrire	WaveResource*		
AssociateApplications	Accorde l'autorisation d'associer des applications à une vague	Écrire	ApplicationResource*		
			WaveResource*		
AssociateSourceServers	Accorde l'autorisation d'associer des serveurs sources à une application	Écrire	ApplicationResource*		
			SourceServerResource*		
BatchCreateVolumeSnapshotGroupForMgn	Accorce l'autorisation de créer un groupe d'instantanés de volume.	Écriture	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
BatchDeleteSnapshotRequestForMgn [autorisation uniquement]	Accorde l'autorisation de supprimer par lot la demande d'instantané.	Écriture			
ChangeServerLifeCycleState	Accorde l'autorisation de modifier l'état du cycle de vie du serveur source.	Écrire	SourceServerResource*		
CreateApplication	Accorde l'autorisation de créer une application	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Accorde l'autorisation de créer un connecteur	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLaunchConfigurationTemplate	Accorde l'autorisation de créer un modèle de configuration du lancement	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkMigrationDefinition	Accorde l'autorisation de créer une définition de migration réseau	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicationConfigurationTemplate	Accorde l'autorisation de créer un modèle de configuration de réplication.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVcenterClientForMgn [autorisation uniquement]	Accorde l'autorisation de créer un client vcenter	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWave	Accorde l'autorisation de créer une vague	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	ApplicationResource*		
DeleteConnector	Accorde l'autorisation de supprimer un connecteur	Écrire	ConnectorResource*		
DeleteJob	Accorde l'autorisation de supprimer la tâche.	Écrire	JobResource*		
DeleteLaunchConfigurationTemplate	Accorde l'autorisation de supprimer le modèle de configuration du lancement	Écrire	LaunchConfigurationTemplateResource*		
DeleteNetworkMigrationDefinition	Autorise la suppression d'une définition de migration réseau	Écrire	NetworkMigrationDefinitionResource*		
DeleteReplicationConfigurationTemplate	Accorde l'autorisation de supprimer un modèle de configuration de réplication.	Écriture	ReplicationConfigurationTemplateResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSourceServer	Accorde l'autorisation de supprimer le serveur source.	Écrire	SourceServerResource*		
DeleteVcenterClient	Accorde l'autorisation de supprimer un client vcenter	Écrire	VcenterClientResource*		
DeleteWave	Accorde l'autorisation de supprimer une vague	Écrire	WaveResource*		
DescribeJobLogItems	Accorde l'autorisation de décrire les éléments du journal des tâches.	Lecture	JobResource*		
DescribeJobs	Accorde l'autorisation de décrire les tâches.	List			
DescribeLaunchConfigurationTemplates	Accorde l'autorisation de décrire le modèle de configuration du lancement	List			
DescribeReplicationConfigurationTemplates	Accorde l'autorisation de décrire le modèle de configuration de réplication.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReplicationServerAssociationsForMgn [autorisation uniquement]	Accorde l'autorisation de décrire les associations de serveur de réplication.	Lecture			
DescribeSnapshotRequestsForMgn [autorisation uniquement]	Accorde l'autorisation de décrire les demandes d'instantanés.	Lecture			
DescribeSourceServers	Accorde l'autorisation de décrire les serveurs source.	List			
DescribeVcenterClients	Accorde l'autorisation de décrire les clients vcenter	List			
DisassociateApplications	Accorde l'autorisation de dissocier les applications d'une vague	Écrire	ApplicationResource*		
			WaveResource*		
DisassociateSourceServers	Accorde l'autorisation de dissocier les serveurs sources d'une application	Écrire	ApplicationResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			SourceServerResource*		
DisconnectFromService	Accorde l'autorisation de déconnecter le serveur source du service.	Écriture	SourceServerResource*		
FinalizeCutover	Accorde l'autorisation de finaliser le basculement.	Écrire	SourceServerResource*		
GetAccountSettings	Accorde l'autorisation d'obtenir les paramètres d'un compte	Lecture			
GetAgentCommandForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir la commande de l'agent.	Lecture	SourceServerResource*		
GetAgentConfirmedResumeInfoForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations de reprise confirmées par l'agent.	Lecture	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAgentInstallationAssetsForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir les ressources d'installation de l'agent.	Lecture			
GetAgentReplicationInfoForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations de réplication de l'agent.	Lecture	SourceServerResource*		
GetAgentRuntimeConfigurationForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir la configuration d'exécution de l'agent.	Lecture	SourceServerResource*		
GetAgentSnapshotCreditsForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir des crédits d'instantanés de l'agent.	Lecture	SourceServerResource*		
GetChannelCommandsForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir des commandes de canal.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLaunchConfiguration	Accorde l'autorisation d'obtenir la configuration de lancement.	Lecture	SourceServerResource*		
GetNetworkMigrationDefinition	Accorde l'autorisation d'obtenir une définition de migration réseau	Lecture	NetworkMigrationDefinitionResource*		
GetNetworkMigrationMapperSegmentConstruct	Accorde l'autorisation d'obtenir la construction d'un segment de mappeur de migration réseau	Lecture	NetworkMigrationDefinitionResource*		
GetReplicationConfiguration	Accorde l'autorisation d'obtenir la configuration de réplication.	Lecture	SourceServerResource*		
GetVcenterClientCommandsForMgn [autorisation uniquement]	Accorde l'autorisation d'obtenir les commandes du client vcenter	Lecture	VcenterClientResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InitializeService	Accorde l'autorisation d'initialiser le service.	Écrire			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueClientCertificateForMgn [autorisation uniquement]	Accorde l'autorisation d'émettre un certificat client	Écrire	SourceServerResource		
ListApplications	Accorde l'autorisation de répertorier les récapitulatifs des applications	List			
ListConnectors	Accorde l'autorisation de répertorier les connecteurs	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListExportErrors	Octroie l'autorisation de répertorier les erreurs d'une tâche d'exportation	List	ExportResource*		
ListExports	Octroie l'autorisation de répertorier les tâches d'exportation	List			
ListImportErrors	Octroie l'autorisation de répertorier les erreurs d'une tâche d'importation	List	ImportResource*		
ListImportFileEnrichments	Accorde l'autorisation de répertorier les tâches d'enrichissement des fichiers d'importation	List			
ListImports	Octroie l'autorisation de répertorier les tâches d'importation	List			
ListManagedAccounts	Accorde l'autorisation de répertorier les comptes gérés	List			
ListNetworkMigrationAnalyses	Permet de répertorier les analyses de migration du réseau	List	NetworkMigrationDefinitionResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNetworkMigrationAnalysisResults	Permet de répertorier les résultats de l'analyse de migration du réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerationSegments	Accorde l'autorisation de répertorier les segments de génération de code de migration réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerations	Accorde l'autorisation de répertorier les générations de code de migration réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDefinitions	Accorde l'autorisation de répertorier les définitions de migration réseau	List			
ListNetworkMigrationDeployedStacks	Accorde l'autorisation de répertorier les piles déployées liées à la migration réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployedStacksDeletions	Accorde l'autorisation de répertorier les suppressions de piles déployées liées à la migration sur le réseau	List	NetworkMigrationDefinitionResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNetworkMigrationDeployments	Accorde l'autorisation de répertorier les déploiements de migration réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationExecutions	Accorde l'autorisation de répertorier les exécutions de migration réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegmentConstructs	Accorde l'autorisation de répertorier les constructions de segments du mappeur de migration réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegments	Autorise à répertorier les segments du mappeur de migration réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMappingUpdates	Autorise à répertorier les mises à jour du mappage de migration du réseau	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMappings	Accorde l'autorisation de répertorier les mappages de migration réseau	List	NetworkMigrationDefinitionResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSourceServerActions	Accorde l'autorisation de répertorier les documents d'action du serveur source	List	SourceServerResource*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture			
ListTemplateActions	Accorde l'autorisation de répertorier les documents d'action du modèle de configuration de lancement	List	LaunchConfigurationTemplateResource*		
ListWaves	Accorde l'autorisation de répertorier les récapitulatifs des vagues	List			
MarkAsArchived	Accorde l'autorisation de marquer le serveur source comme archivé.	Écriture	SourceServerResource*		
NotifyAgentAuthenticationForMgn [autorisation uniquement]	Accorde l'autorisation de signaler l'authentification de l'agent.	Écriture	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
NotifyAgentConnectedForMgn [autorisation uniquement]	Accorde l'autorisation de signaler que l'agent est connecté.	Écriture	SourceServerResource*		
NotifyAgentDisconnectedForMgn [autorisation uniquement]	Accorde l'autorisation de signaler que l'agent est déconnecté.	Écriture	SourceServerResource*		
NotifyAgentReplicationProgressForMgn [autorisation uniquement]	Accorde l'autorisation de signaler la progression de la réplication de l'agent.	Écriture	SourceServerResource*		
NotifyVcenterClientStartedForMgn [autorisation uniquement]	Accorde l'autorisation de notifier le démarrage du client vcenter	Écrire	VcenterClientResource*		
PauseReplication	Accorde l'autorisation d'interrompre une réplication	Écrire	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutSourceServerAction	Accorde l'autorisation de placer un document d'action du serveur source	Écrire	SourceServerResource*		
PutTemplateAction	Accorde l'autorisation de placer le document d'action du modèle de configuration de lancement	Écrire	LaunchConfigurationTemplateResource*		
RegisterAgentForMgn [autorisation uniquement]	Accorde l'autorisation d'enregistrer l'agent.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveSourceServerAction	Accorde l'autorisation de supprimer un document d'action du serveur source	Écrire	SourceServerResource*		
RemoveTemplateAction	Accorde l'autorisation de supprimer un document d'action du modèle de configuration du lancement	Écrire	LaunchConfigurationTemplateResource*		
ResumeReplication	Accorde l'autorisation de reprendre une réplication	Écrire	SourceServerResource*		
RetryDataReplication	Accorde l'autorisation de réessayer la réplication.	Écriture	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendAgentLogsForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer des journaux d'agent.	Écriture	SourceServerResource*		
SendAgentMetricsForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer des métriques d'agent.	Écriture	SourceServerResource*		
SendChannelCommandResultForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer le résultat de la commande de canal.	Écriture			
SendClientLogsForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer des journaux client.	Écriture			
SendClientMetricsForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer des métriques client.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendVcenterClientCommandResultForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer le résultat de la commande du client vcenter	Écrire	VcenterClientResource*		
SendVcenterClientLogsForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer des journaux client vcenter	Écrire	VcenterClientResource*		
SendVcenterClientMetricsForMgn [autorisation uniquement]	Accorde l'autorisation d'envoyer des métriques client vcenter	Écrire	VcenterClientResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartCutover	Accorde l'autorisation de démarrer le basculement.	Écrire	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:TerminateInstances iam:PassRole mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartExport	Octroie l'autorisation de lancer une tâche d'exportation	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeLaunchTemplateVersions mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartImport	Octroie l'autorisation de créer une tâche d'importation	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:ModifyLaunchTemplate mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves mgn:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					mgn:UpdateLaunchConfiguration s3:PutObject
StartImportFileEnrichment	Autorise le lancement de l'enrichissement du fichier d'importation	Écrire			ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartNetworkMigrationAnalysis	Autorise le lancement d'une analyse de migration réseau	Écrire	NetworkMigrationDefinitionResource*		directconnect:DescribeConnections directconnect:DescribeDirectConnectGatewayAssociations directconnect:DescribeDirectConnectGatewayAttachments directconnect:DescribeDirectConnectGateways directconnect:DescribeVirtualGateways

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					directconnect:DescribeVirtualInterfaces ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DeleteNetworkInsightsAnalysis

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DeleteNetworkInsightsPath ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DeleteTags ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeInstances ec2:DescribeIntern

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					etGateways ec2:DescribeManagedPrefixLists ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments ec2:DescribeTransitGatewayConnects ec2:DescribeTransi

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					tGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayVpcAttachments ec2:DescribeTransitGateways ec2:DescribeVpcEndpointServiceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPee

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTablePropagations ec2:SearchTransitGatewayRoutes ec2:StartNetworkIn

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					sightsAnalysis elasticloadbalancing:DescribeListeners elasticloadbalancing:DescribeLoadBalancerAttributes elasticloadbalancing:DescribeLoadBalancers elasticloadbalancing:DescribeRules elasticloadbalancing:DescribeTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					elasticloadbalancing:DescribeTargetGroupAttributes elasticloadbalancing:DescribeTargetGroups elasticloadbalancing:DescribeTargetHealth globalaccelerator:ListAccelerators globalaccelerator:ListCustomRoutingAccelerators

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					globalaccelerator:ListCustomRoutingEndpointGroups globalaccelerator:ListCustomRoutingListeners globalaccelerator:ListCustomRoutingPortMappings globalaccelerator:ListEndpointGroups globalaccelerator:ListListeners network-firewall:D

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					escribeFirewall network-firewall:DescribeFirewallPolicy network-firewall:DescribeResourcePolicy network-firewall:DescribeRuleGroup network-firewall:ListFirewallPolicies network-firewall:ListFirewalls network-firewall:L

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					istRuleGroups tiros:CreateQuery tiros:ExtendQuery tiros:GetQueryAnswer tiros:GetQueryExplanation tiros:GetQueryExtensionAccounts
StartNetworkMigrationCodeGeneration	Autorise le lancement de la génération du code de migration réseau	Écrire	NetworkMigrationDefinitionResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartNetworkMigrationDeployedStacksDeletion	Autorise le lancement de la suppression des piles déployées liées à la migration réseau	Écrire	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:AttachInternetGateway ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DeleteNetworkAcl ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DeleteSnapshot ec2:DeleteSubnet ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DetachInternetGateway ec2:DetachVolume ec2:DisableTransitGatewayRouteTablePropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePr

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					opagation ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitG

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					atewayVpcAttachment ec2:ReleaseAddress ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:SearchTransitGatewayRoutes

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartNetworkMigrationDeployment	Autorise le lancement d'un déploiement de migration réseau	Écrire	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:AttachInternetGateway ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNatGateway ec2:CreateNetworkAcl ec2:CreateNetworkAclEntry ec2:CreateNetworkInsightsPath

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:CreateNetworkInterface ec2:CreateRoute ec2:CreateRouteTable ec2:CreateSecurityGroup ec2:CreateSubnet ec2:CreateTags ec2:CreateTransitGatewayRoute ec2:CreateTransitGatewayRouteTable ec2:CreateTransitG

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					atewayVpcAttachment ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DeleteNetworkInsightsPath ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet ec2:DeleteTransitGateway ec2:DeleteTransitG

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					atewayRoute ec2:DeleteTransitGatewayRouteTable ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DescribeAccountAttributes ec2:DescribeAddresses ec2:DescribeAvailabilityZones

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeCustomerGateways ec2:DescribeEgressOnlyInternetGateways ec2:DescribeHosts ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeInternetGateways ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeManagedPrefixLists ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables ec2:DescribeSecurityGroupRules ec2:DescribeSecurityGroups

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransi

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					tGatewayVpcAttachments ec2:DescribeTransitGateways ec2:DescribeVolumes ec2:DescribeVpcEndpointServiceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeVpnGateways ec2:DetachInternetGateway ec2:DetachVolume ec2:DisableTransitGatewayRouteTablePropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:EnableTransitGatewayRouteTablePropagation ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTableAssociations ec2:GetTransitGatewayRouteTablePropagations

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpc

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					Attachment ec2:ReleaseAddress ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis
StartNetworkMigrationMapping	Accorde l'autorisation de démarrer un mappage de migration réseau	Écrire	NetworkMigrationDefinitionResource*		
StartNetworkMigrationMappingUpdate	Autorise le lancement d'une mise à jour du mappage de migration réseau	Écrire	NetworkMigrationDefinitionResource*		
StartReplication	Accorde l'autorisation de démarrer la réplication	Écrire	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartTest	Accorde l'autorisation de démarrer le test.	Écrire	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:TerminateInstances iam:PassRole mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopReplication	Accorde l'autorisation d'arrêter la réplication	Écrire	SourceServerResource*		
TagResource	Accorde l'autorisation d'attribuer une balise de ressource.	Balisage	ApplicationResource		
			ConnectorResource		
			ExportResource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ImportResource		
			JobResource		
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} mgn:CreateAction aws:TagKeys	
TerminateTargetInstances	Accorde l'autorisation de terminer les instances cibles.	Écrire	SourceServerResource*		ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Unarchive Application	Accorde l'autorisation de désarchiver une application	Écrire	ApplicationResource*		
Unarchive Wave	Accorde l'autorisation de désarchiver une vague	Écrire	WaveResource*		
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	ApplicationResource		
			ConnectorResource		
			JobResource		
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			VcenterClientResource		
			WaveResource		
				aws:TagKeys	
UpdateAccountSettings	Accorde l'autorisation de mettre à jour les paramètres du compte	Écrire			
UpdateAgentBacklogForMgn [autorisation uniquement]	Accorde l'autorisation de mettre à jour le backlog de l'agent.	Écriture	SourceServerResource*		
UpdateAgentConversionInfoForMgn [autorisation uniquement]	Accorde l'autorisation de mettre à jour les informations de conversion de l'agent.	Écriture	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgentReplicationInfoForMgn [autorisation uniquement]	Accorde l'autorisation de mettre à jour les informations de réplication de l'agent.	Écriture	SourceServerResource*		
UpdateAgentReplicationProcessStateForMgn [autorisation uniquement]	Accorde l'autorisation de mettre à jour l'état du processus de réplication de l'agent.	Écriture	SourceServerResource*		
UpdateAgentSourcePropertiesForMgn [autorisation uniquement]	Accorde l'autorisation de mettre à jour les propriétés sources de l'agent.	Écrire	SourceServerResource*		
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écrire	ApplicationResource*		
UpdateConnector	Accorde l'autorisation de mettre à jour un connecteur	Écrire	ConnectorResource*		
UpdateLaunchConfiguration	Accorde l'autorisation de mettre à jour la configuration de lancement.	Écrire	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateLaunchConfigurationTemplate	Accorde l'autorisation de mettre à jour la configuration de lancement.	Écrire	LaunchConfigurationTemplateResource*		
UpdateNetworkMigrationDefinition	Autorise la mise à jour d'une définition de migration réseau	Écrire	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegment	Autorise la mise à jour d'un segment du mappeur de migration réseau	Écrire	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegmentConstruct	Autorise la mise à jour d'une structure de segment du mappeur de migration réseau	Écrire	NetworkMigrationDefinitionResource*		
UpdateReplicationConfiguration	Accorde l'autorisation de mettre à jour la configuration de réplication.	Écriture	SourceServerResource*		
UpdateReplicationConfigurationTemplate	Accorde l'autorisation de mettre à jour le modèle de configuration de réplication.	Écrire	ReplicationConfigurationTemplateResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSourceServer	Accorde l'autorisation de mettre à jour le serveur source	Écrire	SourceServerResource*		
UpdateSourceServerReplicationType	Accorde l'autorisation de mettre à jour le type de réplication du serveur source	Écrire	SourceServerResource*		
UpdateWave	Accorde l'autorisation de mettre à jour une vague	Écrire	WaveResource*		
VerifyClientRoleForMgn [autorisation uniquement]	Accorde l'autorisation de vérifier le rôle du client	Lecture			

Types de ressources définis par le service de migration des AWS applications

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
JobResource	arn:${Partition}:mgn:${Region}:${Account}:job/${JobID}	aws:ResourceTag/${TagKey}
ReplicationConfigurationTemplateResource	arn:${Partition}:mgn:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	arn:${Partition}:mgn:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}	aws:ResourceTag/${TagKey}
VcenterClientResource	arn:${Partition}:mgn:${Region}:${Account}:vcenter-client/${VcenterClientID}	aws:ResourceTag/${TagKey}
SourceServerResource	arn:${Partition}:mgn:${Region}:${Account}:source-server/${SourceServerID}	aws:ResourceTag/${TagKey}
ApplicationResource	arn:${Partition}:mgn:${Region}:${Account}:application/${ApplicationID}	aws:ResourceTag/${TagKey}
WaveResource	arn:${Partition}:mgn:${Region}:${Account}:wave/${WaveID}	aws:ResourceTag/${TagKey}
ImportResource	arn:${Partition}:mgn:${Region}:${Account}:import/${ImportID}	aws:ResourceTag/${TagKey}
ExportResource	arn:${Partition}:mgn:${Region}:${Account}:export/${ExportID}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Connector Resource	`arn:${Partition}:mgn:${Region}:${Account}:connector/${ConnectorID}`	aws:ResourceTag/${TagKey}
NetworkMigrationDefinitionResource	`arn:${Partition}:mgn:${Region}:${Account}:network-migration-definition/${NetworkMigrationDefinitionID}`	aws:ResourceTag/${TagKey}

Clés de condition pour le service de migration d' AWS applications

AWS Le service de migration d'applications définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés de balise dans la demande	ArrayOfString
mgn:CreateAction	Filtre l'accès en fonction du nom d'une action d'API de création de ressources.	String

Actions, ressources et clés de condition pour Amazon Application Recovery Controller - Zonal Shift

Amazon Application Recovery Controller - Zonal Shift (préfixe de service :`arc-zonal-shift`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Application Recovery Controller - Zonal Shift
- Types de ressources définis par Amazon Application Recovery Controller - Zonal Shift
- Clés de condition pour Amazon Application Recovery Controller - Zonal Shift

Actions définies par Amazon Application Recovery Controller - Zonal Shift

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelPracticeRun	Autorise l'annulation d'une séance d'entraînement active	Écrire	ALB*		
			NLB*		
				arc-zonal-shift:Re	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				sourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CancelZonalShift	Accorde l'autorisation d'annuler un changement de zone actif	Écrire	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePracticeRunConfiguration	Octroie l'autorisation de créer une configuration de répétition.	Écrire	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeletePracticeRunConfiguration	Octroie l'autorisation de supprimer une configuration de répétition.	Écrire	ALB*		
			NLB*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetAutoshiftObserverNotificationStatus	Accorde l'autorisation d'obtenir le statut de notification AutoShift Observer	Lecture			
GetManagedResource	Accorde l'autorisation d'obtenir des informations sur une ressource gérée	Lecture	ALB* NLB*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ListAutoshifts	Octroie l'autorisation de répertorier des changements automatiques actifs et terminés.	List			
ListManagedResources	Accorde l'autorisation de répertorier des ressources gérées	List			
ListZonalShifts	Accorde l'autorisation de répertorier les changements de zone	List			
StartPracticeRun	Donne l'autorisation de démarrer une course d'entraînement	Écrire	ALB* NLB*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
StartZonalShift	Accorde l'autorisation de démarrer un changement de zone	Écrire	ALB*		
			NLB*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateAutoshiftObserverNotificationStatus	Accorde l'autorisation de mettre à jour le statut de notification AutoShift Observer	Écrire			
UpdatePracticeRunConfiguration	Octroie l'autorisation de mettre à jour une configuration de répétition.	Écrire	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalAutoshiftConfiguration	Octroie l'autorisation de mettre à jour le statut d'un changement automatique de zone.	Écrire	ALB*		iam:CreateServiceLinkedRole
			NLB*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalShift	Accorde l'autorisation de mettre à jour un changement de zone	Écrire	ALB*		
			NLB*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Types de ressources définis par Amazon Application Recovery Controller - Zonal Shift

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
ALB	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/`	arc-zonal-shift:ResourceIdentifier

Types de ressources	ARN	Clés de condition
	app/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
NLB	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Clés de condition pour Amazon Application Recovery Controller - Zonal Shift

Amazon Application Recovery Controller - Zonal Shift définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
arc-zonal-shift:ResourceIdentifier	Filtre l'accès en fonction de l'identifiant de ressource de la ressource gérée	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des étiquettes associées à la ressource	String
elasticloadbalancing:ResourceTag/${TagKey}	Filtre l'accès en fonction des étiquettes associées à la ressource	String

Actions, ressources et clés de condition pour le service de transformation des AWS applications

AWS Le service de transformation des applications (préfixe de service :`application-transformation`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service de transformation des AWS applications
- Types de ressources définis par le service de transformation des AWS applications
- Clés de condition pour le service de transformation des AWS applications

Actions définies par le service de transformation des AWS applications

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContainerization	Accorde l'autorisation d'obtenir les détails de toutes les tâches de conteneurisation	Lecture			
GetDeployment	Accorde l'autorisation d'obtenir les détails de toutes les tâches de déploiement	Lecture			
GetGroupingAssessment	Accorde l'autorisation d'obtenir les détails d'une opération d'évaluation de groupement	Lecture			
GetPortingCompatibilityAssessment	Accorde l'autorisation d'obtenir l'opération de compatibilité de portage	Lecture			
GetPortingRecommendationAssessment	Accorde l'autorisation d'obtenir les détails d'une opération d'évaluation de la recommandation de portage	Lecture			
GetRuntimeAssessment	Accorde l'autorisation d'obtenir les détails d'une opération d'évaluation de la durée d'exécution	Lecture			
PutLogData	Accorde l'autorisation d'envoyer des journaux (réservé aux clients)	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutMetricData	Accorde l'autorisation d'envoyer des données métriques (réservé aux clients)	Écrire			
StartContainerization	Accorde l'autorisation de démarrer une tâche de conteneurisation	Écrire			
StartDeployment	Octroie l'autorisation de démarrer une tâche de déploiement.	Écrire			
StartGroupingAssessment	Accorde l'autorisation de lancer une opération d'évaluation de groupement	Écrire			
StartPortingCompatibilityAssessment	Accorde l'autorisation de lancer l'opération de compatibilité de portage	Écrire			
StartPortingRecommendationAssessment	Accorde l'autorisation de lancer l'opération d'évaluation de la recommandation de portage	Écrire			
StartRuntimeAssessment	Accorde l'autorisation de lancer une opération d'évaluation de la durée d'exécution	Écrire			

Types de ressources définis par le service de transformation des AWS applications

AWS Le service de transformation des applications ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Application Transformation Service, spécifiez la `"Resource": "*"` dans votre politique.

Clés de condition pour le service de transformation des AWS applications

Application Transformation Service ne comporte pas de clés de contexte propres au service qui puissent être utilisées dans l'élément de `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon AppStream 2.0

Amazon AppStream 2.0 (préfixe de service :`appstream`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon AppStream 2.0
- Types de ressources définis par Amazon AppStream 2.0
- Clés de condition pour Amazon AppStream 2.0

Actions définies par Amazon AppStream 2.0

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAppBlockBuilderAppBlock	Accorde l'autorisation d'associer le générateur de blocs d'applications spécifié au bloc d'applications	Écrire	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationFleet	Accorde l'autorisation d'associer l'application spécifiée à la flotte	Écrire	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
AssociateApplicationToEntitlement	Accorde l'autorisation d'associer l'application spécifiée au droit spécifié	Écrire	stack*		
AssociateFleet	Accorde l'autorisation d'associer la flotte spécifiée à la pile spécifiée	Écrire	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateSoftwareToImageBuilder	Accorde l'autorisation d'associer une ou plusieurs applications incluses dans la licence à une instance de générateur d'images existante	Écrire	image-builder*		
				aws:ResourceTag/${TagKey}	
BatchAssociateUserStack	Accorde l'autorisation d'associer les utilisateurs spécifiés aux piles spécifiées. Les utilisateurs appartenant à un groupe d'utilisateurs ne peuvent pas être affectés à des piles comprenant des parcs joints à un domaine Active Directory	Écriture	stack*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateUserStack	Accorde l'autorisation de dissocier les utilisateurs spécifiés des piles spécifiées	Écrire	stack*		
				aws:ResourceTag/${TagKey}	
CopyImage	Accorde l'autorisation de copier l'image spécifiée dans la même région ou dans une nouvelle région au sein de la même Compte AWS	Écrire	image*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAppBlock	Accorde l'autorisation de créer un bloc d'applications. Les blocs d'applications stockent des informations sur le disque dur virtuel qui contient les fichiers de l'application dans un compartiment S3. Il stocke également le script de configuration avec des instructions sur le montage du disque dur virtuel. Les blocs d'applications sont uniquement pris en charge pour les flottes Elastic.	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilder	Accorde l'autorisation de créer un générateur de blocs d'applications. Le générateur de blocs d'applications est une machine virtuelle utilisée pour créer un bloc d'applications	Écrire	app-block-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilderStreamingURL	Accorde l'autorisation de créer une URL pour lancer une session de streaming du générateur de blocs d'applications	Écrire	app-block-builder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CreateApplication	Accorde l'autorisation de créer une application dans un compte client. Les applications stockent des informations sur la manière de lancer des d'applications sur des instances de streaming. Ceci est uniquement pris en charge pour les flottes Elastic.	Écrire	app-block*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateDirectoryConfig	Accorde l'autorisation de créer un objet Directory Config dans la AppStream version 2.0. Cet objet inclut les informations de configuration requises pour joindre des parcs et des instances Image Builder à des domaines Microsoft Active Directory	Écrire			
CreateEntitlement	Accorde l'autorisation de créer un droit pour contrôler l'accès aux applications en fonction des attributs utilisateur	Écrire	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExportImageTask	Accorde l'autorisation de créer une tâche d'exportation pour une image AppStream 2.0	Écrire		aws:ResourceTag/${TagKey}	
CreateFleet	Accorde l'autorisation de créer un parc. Un parc est un groupe d'instances de streaming à partir duquel les applications sont lancées et diffusées aux utilisateurs	Écriture	fleet*		
			image		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilder	Accorde l'autorisation de créer une instance Image Builder. Une instance Image Builder est une machine virtuelle utilisée pour créer une image	Écriture	image*		
			image-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilderStreamingURL	Accorde l'autorisation de créer une URL pour démarrer une session de streaming Image Builder	Écrire	image-builder*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateImportedImage	Accorde l'autorisation de créer une image AppStream 2.0 à partir d'une AMI importée	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateStack	Accorde l'autorisation de créer une pile pour lancer le streaming d'applications aux utilisateurs. Une pile se compose d'un parc associé, de stratégies d'accès des utilisateurs et de configurations de stockage	Écrire	stack*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamingURL	Accorde l'autorisation de créer une URL temporaire pour démarrer une session de streaming AppStream 2.0 pour l'utilisateur spécifié. Une URL de streaming permet de tester le streaming d'application sans configuration d'un utilisateur	Écrire	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateThemeForStack	Accorde l'autorisation de créer un thème de marque personnalisé, qui peut inclure un logo personnalisé, des liens vers des sites Web et d'autres éléments de marque à afficher auprès de vos utilisateurs	Écrire	stack*		
CreateUpdatedImage	Accorde l'autorisation de mettre à jour une image existante dans le compte client	Écrire	image*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateUsageReportSubscription	Accorde l'autorisation de créer un abonnement au rapport d'utilisation. Les rapports d'utilisation sont générés tous les jours	Écriture			
CreateUser	Accorde l'autorisation de créer un nouvel utilisateur dans le groupe d'utilisateurs	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAppBlock	Accorde l'autorisation de supprimer le bloc d'applications spécifié	Écrire	app-block*		
				aws:ResourceTag/${TagKey}	
DeleteAppBlockBuilder	Accorde l'autorisation de supprimer le générateur de blocs d'applications spécifié et de libérer la capacité	Écrire	app-block-builder*		
				aws:ResourceTag/${TagKey}	
DeleteApplication	Accorde l'autorisation de supprimer l'application spécifiée	Écrire	application*		
				aws:ResourceTag/${TagKey}	
DeleteDirectoryConfig	Accorde l'autorisation de supprimer l'objet Directory Config spécifié à partir de la AppStream version 2.0. Cet objet inclut les informations de configuration requises pour joindre des parcs et des instances Image Builder à des domaines Microsoft Active Directory	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEntitlement	Accorde l'autorisation de supprimer le droit spécifié	Écrire	stack*		
DeleteFleet	Accorde l'autorisation de supprimer le parc spécifié	Écriture	fleet*		
				aws:ResourceTag/${TagKey}	
DeleteImage	Accorde l'autorisation de supprimer l'image spécifiée. Une image ne peut pas être supprimée lorsqu'elle est en cours d'utilisation	Écriture	image*		
				aws:ResourceTag/${TagKey}	
DeleteImageBuilder	Accorde l'autorisation de supprimer l'instance Image Builder spécifiée et de libérer la capacité	Écriture	image-builder*		
				aws:ResourceTag/${TagKey}	
DeleteImagePermissions	Accorde l'autorisation de supprimer les autorisations pour l'image privée spécifiée	Écriture	image*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteStack	Accorde l'autorisation de supprimer la pile spécifiée. Une fois la pile supprimée, l'environnement de streaming d'application fourni par la pile n'est plus accessible aux utilisateurs. De plus, les réservations effectuées pour les sessions de streaming d'application pour la pile sont publiées	Écrire	stack*		
				aws:ResourceTag/${TagKey}	
DeleteThemeForStack	Accorde l'autorisation de supprimer un thème de marque personnalisé, qui peut inclure un logo personnalisé, des liens vers des sites Web et d'autres éléments de marque à afficher auprès de vos utilisateurs	Écrire	stack*		
DeleteUsageReportSubscription	Accorde l'autorisation de désactiver la génération du rapport d'utilisation	Écriture			
DeleteUser	Accorde l'autorisation de supprimer un utilisateur du groupe d'utilisateurs	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAppBlockBuilderAppBlockAssociations	Accorde l'autorisation de récupérer les associations liées au générateur de blocs d'applications ou au bloc d'applications spécifié	List			
DescribeAppBlockBuilders	Accorde l'autorisation de récupérer une liste décrivant un ou plusieurs générateurs de blocs d'applications spécifiés, si les noms des générateurs de blocs d'applications sont fournis. Sinon, tous les générateurs de blocs d'applications du compte sont décrits	List			
DescribeAppBlocks	Accorde l'autorisation de récupérer une liste qui décrit la ou les blocs d'applications spécifiés, si les ARN des blocs d'applications sont fournis. Sinon, tous les blocs d'applications du compte sont décrits	List			
DescribeAppLicenseUsage	Accorde l'autorisation de récupérer les informations d'utilisation des applications incluses dans la licence	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeApplicationFleetAssociations	Accorde l'autorisation de récupérer les associations associées à l'application ou à la flotte spécifiée	List			
DescribeApplications	Accorde l'autorisation de récupérer une liste qui décrit une ou plusieurs applications, si les ARN de l'application sont fournis. Sinon, toutes les applications du compte sont décrits	List			
DescribeDirectoryConfigs	Accorde l'autorisation de récupérer une liste qui décrit un ou plusieurs objets Directory Config spécifiés pour AppStream 2.0, si les noms de ces objets sont fournis. Sinon, tous les objets Directory Config du compte sont décrits. Cet objet inclut les informations de configuration requises pour joindre des parcs et des instances Image Builder à des domaines Microsoft Active Directory	List			
DescribeEntitlements	Accorde l'autorisation de récupérer un ou tous les droits de la pile spécifiée	List	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFleets	Accorde l'autorisation de récupérer une liste qui décrit un ou plusieurs parcs, si les noms des parcs sont fournis. Sinon, tous les parcs du compte sont décrits	List			
DescribeImageBuilders	Accorde l'autorisation de récupérer une liste qui décrit une ou plusieurs instances Image Builders, si les noms de celles-ci sont fournis. Sinon, toutes les instances Image Builders du compte sont décrites	List			
DescribeImagePermissions	Accorde l'autorisation de récupérer une liste qui décrit les autorisations de partage Compte AWS IDs sur une image privée que vous possédez	Lecture	image*		
DescribeImages	Accorde l'autorisation de récupérer une liste qui décrit une ou plusieurs images spécifiées, si les noms ou ARNs les images sont fournis. Sinon, toutes les images du compte sont décrites	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSessions	Accorde l'autorisation de récupérer une liste décrivant les sessions de streaming pour la pile et le parc spécifiés. Si un ID utilisateur est fourni pour la pile et le parc, seules les sessions de streaming pour cet utilisateur sont décrites	List	fleet* stack*		
DescribeSoftwareAssociations	Accorde l'autorisation de récupérer les associations d'applications incluses dans la licence pour une ressource spécifiée	List	image image-builder		
DescribeStacks	Accorde l'autorisation de récupérer une liste qui décrit la ou les piles spécifiées, si les noms de la pile sont fournis. Sinon, toutes les piles du compte sont décrites	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeThemeForStack	Accorde l'autorisation d'obtenir les informations du thème de marque personnalisé, qui peuvent inclure un logo personnalisé, des liens vers des sites Web et d'autres informations de marque à afficher auprès de vos utilisateurs	Lecture	stack*		
DescribeUsageReportSubscriptions	Accorde l'autorisation de récupérer une liste qui décrit un ou plusieurs abonnements au rapport d'utilisation	List			
DescribeUserStackAssociations	Accorde l'autorisation de récupérer une liste qui décrit les UserStackAssociation objets	List			
DescribeUsers	Accorde l'autorisation de récupérer une liste qui décrit les utilisateurs du groupe d'utilisateurs	List			
DisableUser	Accorde l'autorisation de désactiver l'utilisateur spécifié dans le groupe d'utilisateurs. Cette action ne permet pas de supprimer l'utilisateur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateAppBlockBuilderAppBlock	Accorde l'autorisation de dissocier le générateur de blocs d'applications spécifié à partir du bloc d'applications	Écrire	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFleet	Accorde l'autorisation de dissocier l'application spécifiée à partir de la flotte spécifiée	Écrire	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFromEntitlement	Accorde l'autorisation de dissocier l'application spécifiée à partir du droit spécifié	Écrire	stack*		
DisassociateFleet	Accorde l'autorisation de dissocier le parc spécifié à partir de la pile spécifiée	Écrire	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateSoftwareFromImageBuilder	Accorde l'autorisation de supprimer les associations d'applications incluses dans la licence d'une instance de générateur d'images	Écrire	image-builder*		
				aws:ResourceTag/${TagKey}	
EnableUser	Accorde l'autorisation d'activer un utilisateur dans le groupe d'utilisateurs	Écriture			
ExpireSession	Accorde l'autorisation d'arrêter immédiatement la session de streaming spécifiée	Écrire			
GetExportImageTask	Accorde l'autorisation de récupérer les détails d'une tâche d'exportation d'image spécifique	Lecture			
ListAssociatedFleets	Accorde l'autorisation de récupérer le nom du parc associé à la pile spécifiée	Lecture	stack*		
ListAssociatedStacks	Accorde l'autorisation de récupérer le nom de la pile à laquelle le parc spécifié est associé	Lecture	fleet*		
ListEntitledApplications	Accorde l'autorisation de récupérer les applications associées au droit spécifié	List	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListExportImageTasks	Accorde l'autorisation de répertorier les tâches d'exportation d'images	List			
ListTagsForResource	Accorde l'autorisation de récupérer une liste de toutes les balises pour la ressource AppStream 2.0 spécifiée. Les ressources suivantes peuvent être balisées : des instances Image Builders, des images, des parcs et des piles	Lecture			
StartAppBlockBuilder	Accorde l'autorisation de démarrer le générateur de blocs d'applications spécifié	Écrire	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StartFleet	Accorde l'autorisation de lancer le parc spécifié	Écriture	fleet*		
				aws:ResourceTag/${TagKey}	
StartImageBuilder	Accorde l'autorisation de lancer l'instance Image Builder spécifiée	Écrire	image-builder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
StartSoftwareDeploymentToImageBuilder	Accorde l'autorisation de lancer le déploiement d'applications sous licence sur une instance de générateur d'images	Écrire	image-builder*		
				aws:ResourceTag/${TagKey}	
StopAppBlockBuilder	Accorde l'autorisation d'arrêter le générateur de blocs d'applications spécifié	Écrire	app-block-builder*		
				aws:ResourceTag/${TagKey}	
StopFleet	Accorde l'autorisation d'arrêter le parc spécifié	Écriture	fleet*		
				aws:ResourceTag/${TagKey}	
StopImageBuilder	Accorde l'autorisation d'arrêter l'instance Image Builder spécifiée	Écriture	image-builder*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Stream	Accorde l'autorisation aux utilisateurs fédérés de se connecter à l'aide de leurs informations d'identification existantes et de diffuser des applications à partir de la pile spécifiée	Écrire	stack*		
				appstream:userId	
TagResource	Accorde l'autorisation d'ajouter ou de remplacer une ou plusieurs balises pour la ressource AppStream 2.0 spécifiée. Les ressources suivantes peuvent être balisées : des instances Image Builders, des images, des flottes, des piles, des blocs d'applications et des applications	Identification	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de dissocier une ou plusieurs balises de la ressource AppStream 2.0 spécifiée	Identification	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAppBlockBuilder	Accorde l'autorisation de mettre à jour le générateur de blocs d'applications spécifié. Le générateur de blocs d'applications est une machine virtuelle utilisée pour créer un bloc d'applications	Écrire	app-block-builder*		
				aws:ResourceTag/${TagKey}	
UpdateApplication	Accorde l'autorisation de mettre à jour les champs spécifiés pour l'application spécifiée	Écrire	application*		
			app-block		
				aws:ResourceTag/${TagKey}	
UpdateDirectoryConfig	Accorde l'autorisation de mettre à jour l'objet Directory Config spécifié dans la AppStream version 2.0. Cet objet inclut les informations de configuration requises pour joindre des parcs et des instances Image Builder à des domaines Microsoft Active Directory	Écrire			
UpdateEntitlement	Accorde l'autorisation de mettre à jour les champs spécifiés pour le droit spécifié	Écrire	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFleet	Accorde l'autorisation de mettre à jour le parc spécifié. Tous les attributs, à l'exception du nom du parc peuvent être mis à jour lorsque le parc est à l'état STOPPED (ARRÊTÉ)	Écriture	fleet*		
			image		
				aws:ResourceTag/${TagKey}	
UpdateImagePermissions	Accorde l'autorisation d'ajouter ou de mettre à jour les autorisations pour l'image privée spécifiée	Écriture	image*		
				aws:ResourceTag/${TagKey}	
UpdateStack	Accorde l'autorisation de mettre à jour les champs spécifiés pour la pile spécifiée	Écrire	stack*		
				aws:ResourceTag/${TagKey}	
UpdateThemeForStack	Accorde l'autorisation de mettre à jour les informations du thème de marque personnalisé, qui peuvent inclure un logo personnalisé, des liens vers des sites Web et d'autres informations de marque à afficher auprès de vos utilisateurs	Écrire	stack*		

Types de ressources définis par Amazon AppStream 2.0

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
fleet	`arn:${Partition}:appstream:${Region}:${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:appstream:${Region}:${Account}:image/${ImageName}`	aws:ResourceTag/${TagKey}
image-builder	`arn:${Partition}:appstream:${Region}:${Account}:image-builder/${ImageBuilderName}`	aws:ResourceTag/${TagKey}
stack	`arn:${Partition}:appstream:${Region}:${Account}:stack/${StackName}`	aws:ResourceTag/${TagKey}
app-block	`arn:${Partition}:appstream:${Region}:${Account}:app-block/${AppBlockName}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:appstream:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}
app-block-builder	`arn:${Partition}:appstream:${Region}:${Account}:app-block-builder/${AppBlockBuilderName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon AppStream 2.0

Amazon AppStream 2.0 définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
appstream:userId	Filtre l'accès en fonction de l'ID de l'utilisateur AppStream 2.0	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS AppSync

AWS AppSync (préfixe de service :`appsync`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS AppSync
- Types de ressources définis par AWS AppSync
- Clés de condition pour AWS AppSync

Actions définies par AWS AppSync

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateApi	Accorde l'autorisation d'associer une API GraphQL à un nom de domaine personnalisé dans AppSync	Écrire	domain*		
AssociateMergedGraphqlApi	Accorde l'autorisation d'associer une API fusionnée à une API source.	Écrire	graphqlapi*		
AssociateSourceGraphqlApi	Accorde l'autorisation d'associer une API source à une API fusionnée.	Écrire	graphqlapi*		
AssociateWebACL [autorisation uniquement]	Accorde l'autorisation d'associer une ACL Web à une ressource	Écrire	api		
			graphqlapi		
CreateApi	Accorde l'autorisation de créer une API	Écrire		aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApiCache	Accorde l'autorisation de créer un cache d'API dans AppSync	Écrire			
CreateApiKey	Accorde l'autorisation de créer une clé unique que vous pouvez distribuer aux clients qui exécutent votre API	Écrire			
CreateChannelNamespace	Autorise la création d'un espace de noms de chaîne	Écrire	channelNamespace*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Accorde l'autorisation de créer une source de données.	Écrire			
CreateDomainName		Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de créer un nom de domaine personnalisé dans AppSync			aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	Accorde l'autorisation de créer une fonction	Écrire			
CreateGraphqlApi	Accorde l'autorisation de créer une API GraphQL, qui est la ressource de premier niveau AppSync	Écrire		aws:RequestTag/${TagKey} aws:TagKeys appsync:Visibility	iam:CreateServiceLinkedRole
CreateResolver	Accorde l'autorisation de créer un résolveur. Un résolveur convertit les demandes entrantes dans un format qu'une source de données peut comprendre, et convertit les réponses de la source de données en GraphQL	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateType	Accorde l'autorisation de créer un type	Écrire			
DeleteApi	Accorde l'autorisation de supprimer une API. Cela nettoiera également toutes les AppSync ressources situées en dessous de cette API	Écrire	api*		
				aws:ResourceTag/${TagKey}	
DeleteApiCache	Accorde l'autorisation de supprimer un cache d'API dans AppSync	Écrire			
DeleteApiKey	Accorde l'autorisation de supprimer une clé d'API	Écrire			
DeleteChannelNamespace	Autorise la suppression de l'espace de noms d'une chaîne	Écrire	channelNamespace*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Accorde l'autorisation de supprimer une source de données.	Écrire			
DeleteDomainName	Accorde l'autorisation de supprimer un nom de domaine personnalisé dans AppSync	Écrire	domain*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFunction	Accorde l'autorisation de supprimer une fonction	Écrire			
DeleteGraphqlApi	Accorde l'autorisation de supprimer une API GraphQL. Cela nettoiera également toutes les AppSync ressources situées en dessous de cette API	Écrire	graphqlapi*		
				aws:ResourceTag/${TagKey}	
DeleteResolver	Accorde l'autorisation de supprimer un résolveur	Écrire			
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer une stratégie de ressources.	Écrire			
DeleteType	Accorde l'autorisation de supprimer un type	Écrire			
DisassociateApi	Accorde l'autorisation de détacher une API GraphQL d'un nom de domaine personnalisé dans AppSync	Écrire	domain*		
DisassociateMergedGraphqlApi	Accorde l'autorisation de supprimer une API source associée d'une API fusionnée identifiée par l'API source.	Écrire	mergedApiAssociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateSourceGraphqlApi	Accorde l'autorisation de supprimer une API source associée d'une API fusionnée identifiée par l'API fusionnée.	Écrire	sourceApiAssociation*		
DisassociateWebACL [autorisation uniquement]	Accorde l'autorisation de dissocier une ACL Web et une ressource	Écrire	api graphqlapi		
EvaluateCode	Accorde l'autorisation d'évaluer le code à l'aide d'une durée d'exécution et d'un contexte	Lecture			
EvaluateMappingTemplate	Accorde l'autorisation d'évaluer le mappage de modèle	Lecture			
EventConnect	Accorde l'autorisation de se connecter à une API d'événement	Écrire	api*		
EventPublish	Autorise la publication d'événements dans l'espace de noms d'une chaîne	Écrire	channelNamespace*		
EventSubscribe	Accorde l'autorisation de s'abonner à un espace de noms de chaîne	Écrire	channelNamespace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
FlushApiCache	Accorde l'autorisation de vider le cache d'une API AppSync	Écrire			
GetApi	Accorde l'autorisation de récupérer une API	Lecture	api*		
				aws:ResourceTag/${TagKey}	
GetApiAssociation	Accorde l'autorisation de lire les détails de l'association entre le nom de domaine personnalisé et l'API GraphQL dans AppSync	Lecture	domain*		
GetApiCache	Accorde l'autorisation de lire les informations relatives à un cache d'API dans AppSync	Lecture			
GetChannelNamespace	Accorde l'autorisation de récupérer l'espace de noms d'une chaîne	Lecture	channelNamespace*		
				aws:ResourceTag/${TagKey}	
GetDataSource	Accorde l'autorisation de récupérer une source de données	Lecture			
GetDataSourceIntrospection	Octroie l'autorisation de récupérer une introspection de source de données.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDomainName	Accorde l'autorisation de lire les informations relatives à un nom de domaine personnalisé dans AppSync	Lecture	domain*		
				aws:ResourceTag/${TagKey}	
GetFunction	Accorde l'autorisation de récupérer une fonction	Lecture			
GetGraphqlApi	Accorde l'autorisation de récupérer une API GraphQL	Lecture	graphqlapi*		
				aws:ResourceTag/${TagKey}	
GetGraphqlApiEnvironmentVariables	Accorde l'autorisation de récupérer les variables d'environnement pour une API GraphQL	Lecture			
GetIntrospectionSchema	Accorde l'autorisation de récupérer le schéma d'introspection d'une API GraphQL	Lecture			
GetResolver	Accorde l'autorisation de récupérer un résolveur	Lecture			
GetResourcePolicy [autorisation uniquement]	Accorde l'autorisation de lire une stratégie de ressources.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSchemaCreationStatus	Accorde l'autorisation de récupérer le statut actuel d'une opération de création de schéma	Lecture			
GetSourceApiAssociation	Accorde l'autorisation de lire les informations relatives à une API source associée à une API fusionnée.	Lecture	sourceApiAssociation*		
GetType	Accorde l'autorisation de récupérer un type	Lecture			
GetWebACLForResource [autorisation uniquement]	Accorde l'autorisation d'obtenir le site Web associé ACLs à une ressource	Lecture	api		
			graphqlapi		
GraphQL [autorisation uniquement]	Accorde l'autorisation d'envoyer une requête GraphQL à une API GraphQL	Écrire	field*		
			graphqlapi*		
ListApiKeys	Accorde l'autorisation de répertorier les clés d'une API donnée	List			
ListApis	Accorde l'autorisation de mettre en vente APIs	List		aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListChannelNamespaces	Accorde l'autorisation de répertorier l'espace de noms des chaînes	List	api*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Accorde l'autorisation de répertorier les sources de données d'une API donnée	List			
ListDomainNames	Accorde l'autorisation d'énumérer des noms de domaine personnalisés dans AppSync	List		aws:ResourceTag/${TagKey}	
ListFunctions	Accorde l'autorisation de répertorier les fonctions d'une API donnée	List			
ListGraphqlApis	Accorde l'autorisation de répertorier GraphQL APIs	List			
ListResolvers	Accorde l'autorisation de répertorier les résolveurs d'une API et d'un type donnés	List			
ListResolversByFunction	Accorde l'autorisation de répertorier les résolveurs associés à une fonction spécifique	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourcesForWebACL [autorisation uniquement]	Accorde l'autorisation d'obtenir des ressources associées pour une ACL Web	List			
ListSourceApiAssociations	Accorde l'autorisation de répertorier les sources APIs associées à une API fusionnée donnée	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:ResourceTag/${TagKey}	
ListTypes	Accorde l'autorisation de répertorier les types d'une API donnée	List			
ListTypesByAssociation	Accorde l'autorisation de répertorier les types d'une association d'API fusionnée et d'API source données.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutGraphqlApiEnvironmentVariables	Accorde l'autorisation de mettre à jour les variables d'environnement pour une API GraphQL	Écrire			
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de définir une stratégie de ressources.	Écrire			
SetWebACL	Accorde l'autorisation de définir une liste ACL web	Gestion des autorisations			
SourceGraphQL [autorisation uniquement]	Accorde l'autorisation d'envoyer une requête GraphQL à une API source d'une API fusionnée.	Écrire	field* graphqlapi*		
StartDataSourceIntrospection	Octroie l'autorisation de procéder à l'introspection d'une source de données.	Écrire			
StartSchemaCreation	Accorde l'autorisation d'ajouter un nouveau schéma à votre API GraphQL. Cette opération est asynchrone : elle GetSchemaCreationStatus peut s'afficher lorsqu'elle est terminée	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartSchemaMerge	Accorde l'autorisation de lancer une fusion de schémas pour une API fusionnée donnée et l'API source associée.	Écrire	sourceApiAssociation*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	api		
			channelNamespace		
			domain		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			graphqlapi		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApi	Accorde l'autorisation de mettre à jour une API	Écrire	api*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateApiCache	Accorde l'autorisation de mettre à jour un cache d'API dans AppSync	Écrire			
UpdateApiKey	Accorde l'autorisation de mettre à jour la clé d'une API donnée	Écrire			
UpdateChannelNamespace	Autorise la mise à jour de l'espace de noms d'une chaîne	Écrire	channelNamespace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataSource	Accorde l'autorisation de mettre à jour une source de données	Écrire			
UpdateDomainName	Accorde l'autorisation de mettre à jour un nom de domaine personnalisé dans AppSync	Écrire	domain*		
				aws:ResourceTag/${TagKey}	
UpdateFunction	Accorde l'autorisation de mettre à jour une fonction existante	Écrire			
UpdateGraphqlApi	Accorde l'autorisation de mettre à jour une API GraphQL	Écrire	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateResolver	Accorde l'autorisation de mettre à jour un résolveur	Écrire			
UpdateSourceApiAssociation	Accorde l'autorisation de mettre à jour l'association d'une API fusionnée et d'une API source.	Écrire	sourceApiAssociation*		
UpdateType	Accorde l'autorisation de mettre à jour un type	Écrire			

Types de ressources définis par AWS AppSync

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
datasource	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/datasources/${DatasourceName}`	
domain	`arn:${Partition}:appsync:${Region}:${Account}:domainnames/${DomainName}`	aws:ResourceTag/${TagKey}
graphqlapi	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}`	aws:ResourceTag/${TagKey}
field	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}/fields/${FieldName}`	
type	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}`	
function	`arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/functions/${FunctionId}`	
sourceApiAssociation	`arn:${Partition}:appsync:${Region}:${Account}:apis/${MergedGraphQLAPIId}/sourceApiAssociations/${Associationid}`	

Types de ressources	ARN	Clés de condition
mergedApiAssociation	arn:${Partition}:appsync:${Region}:${Account}:apis/${SourceGraphQLAPIId}/mergedApiAssociations/${Associationid}	
api	arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}	aws:ResourceTag/${TagKey}
channelNamespace	arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}/channelNamespace/${ChannelNamespaceName}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS AppSync

AWS AppSync définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
appsync:Visibility	Filtre l'accès en fonction de la visibilité d'une API	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identif ication dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le changement de région Amazon ARC

Le commutateur de région Amazon ARC (préfixe de service :`arc-region-switch`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le commutateur de région Amazon ARC
- Types de ressources définis par le commutateur de région Amazon ARC
- Clés de condition pour le changement de région Amazon ARC

Actions définies par le commutateur de région Amazon ARC

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApprovePlanExecutionStep	Accorde l'autorisation d'approuver une étape d'exécution du plan	Écrire	plan*		
CancelPlanExecution	Autorise l'annulation de l'exécution d'un plan	Écrire	plan*		
CreatePlan	Accorde l'autorisation de créer un plan	Écrire	plan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePlan	Autorise la suppression d'un plan	Écrire	plan*		
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer la politique de contrôle d'accès à la RAM pour un plan	Gestion des autorisations			
GetPlan	Accorde l'autorisation d'obtenir des informations sur les plans dans tous les cas à Régions AWS l'aide d'un plan de contrôle	Lecture	plan*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPlanEvaluationStatus	Donne l'autorisation d'obtenir le statut d'évaluation d'un plan	Lecture	plan*		
GetPlanExecution	Accorde l'autorisation d'obtenir les détails d'exécution du plan et les informations de configuration	Lecture	plan*		
GetPlanInRegion	Permet d'obtenir des informations sur un plan spécifique à Région AWS l'aide du changement de région (plan de données régional)	Lecture	plan*		
GetResourcePolicy [autorisation uniquement]	Accorde l'autorisation d'obtenir la politique de ressources d'un plan	Gestion des autorisations	plan*		
ListPlanExecutionEvents	Accorde l'autorisation de répertorier les événements d'exécution du plan	List	plan*		
ListPlanExecutions	Donne l'autorisation de répertorier les exécutions de plans	List	plan*		
ListPlans	Permet de répertorier tous les plans à Régions AWS l'aide d'un plan de contrôle	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPlansInRegion	Permet de répertorier les plans dans un plan spécifique à Région AWS l'aide du changement de région (plan de données régional)	List			
ListRoute53HealthChecks	Autorise à répertorier les bilans de santé de la Route 53	List	plan*		
ListRoute53HealthChecksInRegion	Permet de répertorier les bilans de santé de la Route 53 dans un dossier spécifique à Région AWS l'aide du changement de région (plan de données régional)	List	plan*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	plan*		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de définir la politique de contrôle d'accès à la RAM pour un plan	Gestion des autorisations			
StartPlanExecution	Accorde l'autorisation de démarrer l'exécution d'un plan	Écrire	plan*		
TagResource	Accorde l'autorisation de baliser une ressource	Identification	plan*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	plan*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePlan	Autorise la mise à jour d'un plan	Écrire	plan*		
UpdatePlanExecution	Autorise la mise à jour de l'exécution d'un plan	Écrire	plan*		
UpdatePlanExecutionStep	Autorise la mise à jour d'une étape d'exécution du plan	Écrire	plan*		

Types de ressources définis par le commutateur de région Amazon ARC

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
plan	`arn:${Partition}:arc-region-switch::${Account}:plan/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour le changement de région Amazon ARC

Le commutateur de région Amazon ARC définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Artifact

AWS Artifact (préfixe de service :`artifact`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Artifact
- Types de ressources définis par AWS Artifact
- Clés de condition pour AWS Artifact

Actions définies par AWS Artifact

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptAgreement	Accorde l'autorisation d'accepter un AWS accord qui n'a pas encore été accepté par le compte client	Écrire	agreement *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptNdaForAgreement	Accorde l'autorisation d'accepter les termes d'un document NDA pour une ressource d'accord donnée	Écrire	agreement*		
GetAccountSettings	Octroie l'autorisation d'obtenir les paramètres du compte pour Artifact.	Lecture			
GetAgreement	Permet d'obtenir un AWS accord qui n'a pas encore été accepté par le compte client	Lecture	agreement*		
GetCustomerAgreement	Accorde l'autorisation d'obtenir un AWS accord qui a été accepté par le compte client	Lecture	customer-agreement*		
GetNdaForAgreement	Accorde l'autorisation de récupérer le document NDA pour une ressource d'accord donnée	Lecture	agreement*		
GetReport	Accorde l'autorisation de télécharger un rapport	Lecture	report*		
GetReportMetadata	Accorde l'autorisation de télécharger les métadonnées associées à un rapport	Lecture	report*		
GetTermForReport	Accorde l'autorisation de télécharger un terme associé à un rapport	Lecture	report*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAgreements	Donne l'autorisation de répertorier AWS les accords	List			
ListCustomerAgreements	Accorde l'autorisation de répertorier les ressources liées à un accord client qui ont été acceptées par le compte client	List			
ListReportVersions	Accorde l'autorisation de répertorier les versions des rapports dans votre compte	List			
ListReports	Accorde l'autorisation de répertorier les rapports de votre compte	List			
PutAccountSettings	Octroie l'autorisation de saisir les paramètres du compte pour Artifact.	Écrire			
TerminateAgreement	Accorde l'autorisation de résilier un contrat client qui a été précédemment accepté par le compte client	Écrire	customer-agreement*		

Types de ressources définis par AWS Artifact

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
customer-agreement	`arn:${Partition}:artifact::${Account}:customer-agreement/*`	
agreement	`arn:${Partition}:artifact:::agreement/*`	
report	`arn:${Partition}:artifact:${Region}::report/${ReportId}:${Version}`	artifact:ReportCategory artifact:ReportSeries

Clés de condition pour AWS Artifact

AWS Artifact définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
artifact:ReportCategory	Filtre l'accès en fonction des catégories auxquelles les rapports sont associés	String
artifact:ReportSeries	Filtre l'accès en fonction des séries auxquelles les rapports sont associés	String

Actions, ressources et clés de condition pour Amazon Athena

Amazon Athena (préfixe de service : `athena`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Athena
- Types de ressources définis par Amazon Athena
- Clés de condition pour Amazon Athena

Actions définies par Amazon Athena

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetNamedQuery	Accorde l'autorisation nécessaire pour obtenir des informations relatives à une ou plusieurs requêtes nommées	Lecture	workgroup *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetPreparedStatement	Accorde l'autorisation d'obtenir des informations sur une ou plusieurs instructions préparées	Lecture	workgroup*		
BatchGetQueryExecution	Accorde l'autorisation nécessaire pour obtenir des informations relatives à une ou plusieurs exécutions de requête	Lecture	workgroup*		
CancelCapacityReservation	Accorde l'autorisation d'annuler une réservation de capacité	Écrire	capacity-reservation*		
CancelQueryExecution	Accorde l'autorisation d'annuler l’exécution d’une requête. Obsolète. S'applique uniquement aux AWS services et aux principaux qui utilisent le pilote Athena JDBC antérieur à la version 1.1.0. Utiliser StopQueryExecution autrement	Écrire	workgroup*		
CreateCapacityReservation	Accorde l'autorisation de créer une réservation de capacité	Écrire	capacity-reservation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataCatalog	Accorde l'autorisation nécessaire pour créer un catalogue de données	Écrire	datacatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	Accorde l'autorisation nécessaire pour créer une requête nommée	Écrire	workgroup*		
CreateNotebook	Accorde l'autorisation de créer un bloc-notes	Écrire	workgroup*		
CreatePreparedStatement	Accorde l'autorisation nécessaire pour créer une déclaration préparée	Écrire	workgroup*		
CreatePresignedNotebookUrl	Accorde l'autorisation de créer une URL de bloc-notes présignée	Écrire	workgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkGroup	Accorde l'autorisation nécessaire pour créer un groupe de travail	Écrire	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCapacityReservation	Accorde l'autorisation de supprimer une réserve de capacité	Écrire	capacity-reservation*		
DeleteDataCatalog	Accorde l'autorisation nécessaire pour supprimer un catalogue de données	Écrire	datacatalog*		
DeleteNamedQuery	Accorde l'autorisation nécessaire pour supprimer une requête nommée spécifiée	Écrire	workgroup*		
DeleteNotebook	Accorde l'autorisation de supprimer un bloc-notes	Écrire	workgroup*		
DeletePreparedStatement	Accorde l'autorisation nécessaire pour supprimer une déclaration préparée spécifiée	Écrire	workgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteWorkGroup	Accorde l'autorisation nécessaire pour supprimer un groupe de travail	Écrire	workgroup*		
ExportNotebook	Accorde l'autorisation d'exporter un bloc-notes	Écrire	workgroup*		
GetCalculationExecution	Accorde l'autorisation d'obtenir l'exécution d'un calcul	Lecture	workgroup*		
GetCalculationExecutionCode	Accorde l'autorisation d'obtenir un code d'exécution de calcul	Lecture	workgroup*		
GetCalculationExecutionStatus	Accorde l'autorisation d'obtenir le statut d'exécution d'un calcul	Lecture	workgroup*		
GetCapacityAssignmentConfiguration	Accorde l'autorisation d'obtenir des informations d'attribution de capacité pour une réservation de capacité	Lecture	capacity-reservation*		
GetCapacityReservation	Accorde l'autorisation d'obtenir une réservation de capacité	Lecture	capacity-reservation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCatalogs	Accorde l'autorisation pour permettre l'accès aux bases de données et aux tables. S'applique uniquement aux AWS services gérés, à la politique et aux principes qui utilisent un pilote Athena JDBC version 1.1.0	Lecture			
GetDataCatalog	Accorde l'autorisation nécessaire pour obtenir un catalogue de données	Lecture	datacatalog*		
GetDatabase	Accorde l'autorisation nécessaire pour obtenir une base de données pour un catalogue de données en particulier	Lecture	datacatalog*		
GetExecutionEngine	Accorde l'autorisation pour permettre l'accès aux bases de données et aux tables spécifiées. S'applique uniquement aux AWS services gérés, à la politique et aux principes qui utilisent un pilote Athena JDBC version 1.1.0	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExecutionEngines	Accorde l'autorisation pour permettre l'accès aux bases de données et aux tables. S'applique uniquement aux AWS services gérés, à la politique et aux principes qui utilisent un pilote Athena JDBC version 1.1.0	Lecture			
GetNamedQuery	Accorde l'autorisation nécessaire pour obtenir des informations relatives à la requête nommée spécifiée	Lecture	workgroup *		
GetNamespace	Accorde l'autorisation pour permettre l'accès aux bases de données et aux tables spécifiées. S'applique uniquement aux AWS services gérés, à la politique et aux principes qui utilisent un pilote Athena JDBC version 1.1.0	Lecture			
GetNamespaces	Accorde l'autorisation pour permettre l'accès aux bases de données et aux tables. S'applique uniquement aux AWS services gérés, à la politique et aux principes qui utilisent un pilote Athena JDBC version 1.1.0	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetNotebookMetadata	Accorde l'autorisation d'obtenir les métadonnées du bloc-notes	Lecture	workgroup *		
GetPreparedStatement	Accorde l'autorisation nécessaire pour obtenir des informations relatives à la déclaration préparée spécifiée	Lecture	workgroup *		
GetQueryExecution	Accorde l'autorisation nécessaire pour obtenir des informations relatives à l'exécution de la requête spécifiée	Lecture	workgroup *		
GetQueryExecutions	Accorde l'autorisation d'obtenir des exécutions de requêtes. Obsolète. S'applique uniquement aux AWS services et aux principaux qui utilisent le pilote Athena JDBC antérieur à la version 1.1.0. Utiliser ListQueryExecutions autrement	Lecture			
GetQueryResults	Accorde l'autorisation nécessaire pour obtenir les résultats de la requête	Lecture	workgroup *		
GetQueryResultsStream	Accorde l'autorisation nécessaire pour obtenir le flux de résultats de la requête	Lecture	workgroup *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQueryRuntimeStatistics	Accorde l'autorisation d'obtenir des statistiques d'exécution pour l'exécution de la requête spécifiée	Lecture	workgroup *		
GetResourceDashboard	Accorde l'autorisation d'obtenir une UI/Persistence interface utilisateur dynamique pour une session	Lecture	workgroup *		
			session		
GetSession	Accorde l'autorisation d'obtenir une session	Lecture	workgroup *		
			session		
GetSessionEndpoint	Accorde l'autorisation d'obtenir un point de terminaison de connexion et un jeton d'authentification pour un identifiant de session donné	Écrire	workgroup *		
			session		
GetSessionStatus	Accorde l'autorisation d'obtenir un statut de session	Lecture	workgroup *		
			session		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTable	Accorde l'autorisation pour permettre l'accès à la table spécifiée. S'applique uniquement aux AWS services gérés, à la politique et aux principes qui utilisent un pilote Athena JDBC version 1.1.0	Lecture			
GetTableMetadata	Accorde l'autorisation nécessaire pour obtenir une métadonnée sur une table pour un catalogue de données en particulier	Lecture	datacatalog*		
GetTables	Accorde l'autorisation pour activer l'accès aux tables. S'applique uniquement aux AWS services gérés, à la politique et aux principes qui utilisent un pilote Athena JDBC version 1.1.0	Lecture			
GetWorkGroup	Accorde l'autorisation nécessaire pour obtenir un groupe de travail	Lecture	workgroup*		
ImportNotebook	Accorde l'autorisation d'importer un bloc-notes	Écrire	workgroup*		
ListApplicationDPUSizes	Autorise le renvoi d'une liste de ApplicationRuntimeIds	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCalculationExecutions	Accorde l'autorisation de renvoyer une liste d'exécutions de calculs	List	workgroup*		
ListCapacityReservations	Accorde l'autorisation de renvoyer une liste des réservations de capacité pour la capacité spécifiée Compte AWS	List			
ListDataCatalogs	Accorde l'autorisation de renvoyer une liste de catalogues de données pour le fichier spécifié Compte AWS	List			
ListDatabases	Accorde l'autorisation nécessaire pour renvoyer une liste de bases de données pour un catalogue de données en particulier	List	datacatalog*		
ListEngineVersions	Accorde l'autorisation de renvoyer une liste des versions du moteur Athena pour le moteur spécifié Compte AWS	Lecture			
ListExecutors	Accorde l'autorisation de renvoyer une liste d'exécuteurs	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNamedQueries	Accorde l'autorisation de renvoyer une liste de requêtes nommées dans Amazon Athena pour les requêtes spécifiées Compte AWS	List	workgroup*		
ListNotebookMetadata	Accorde l'autorisation de renvoyer une liste de blocs-notes pour un groupe de travail donné	List	workgroup*		
ListNotebookSessions	Accorde l'autorisation de renvoyer une liste de sessions pour un bloc-notes donné	List	workgroup*		
ListPreparedStatements	Accorde l'autorisation nécessaire pour renvoyer une liste de déclarations préparées pour le groupe de travail spécifié	List	workgroup*		
ListQueryExecutions	Accorde l'autorisation de renvoyer une liste des exécutions de requêtes pour le paramètre spécifié Compte AWS	Lecture	workgroup*		
ListSessions	Accorde l'autorisation de renvoyer une liste de sessions pour un groupe de travail donné	List	workgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTableMetadata	Accorde les autorisations pour renvoyer une liste de métadonnées de table dans une base de données pour un catalogue de données en particulier	Lecture	datacatalog*		
ListTagsForResource	Accorde l'autorisation de renvoyer une liste d'étiquettes pour une ressource	Lecture	capacity-reservation*		
			datacatalog*		
			session*		
			workgroup*		
ListWorkGroups	Accorde l'autorisation de renvoyer une liste de groupes de travail pour le groupe spécifié Compte AWS	List			
PutCapacityAssignmentConfiguration	Accorde l'autorisation d'attribuer une capacité à des requêtes à partir d'une réservation de capacité	Écrire	capacity-reservation*		
			workgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RunQuery	Accorde l'autorisation d'exécuter une requête. Obsolète. S'applique uniquement aux AWS services et aux principaux qui utilisent le pilote Athena JDBC antérieur à la version 1.1.0. Utiliser StartQueryExecution autrement	Écrire			
StartCalculationExecution	Accorde l'autorisation de démarrer une exécution de calcul	Écrire	workgroup *		
StartQueryExecution	Accorde l'autorisation nécessaire pour commencer l'exécution d'une requête à l'aide d'une requête SQL fournie en tant que chaîne	Écrire	workgroup *		
StartSession	Accorde l'autorisation de démarrer une session	Écrire	workgroup *		
			session		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopCalculationExecution	Accorde l'autorisation d'arrêter une exécution de calcul	Écrire	workgroup*		
StopQueryExecution	Accorde l'autorisation nécessaire pour arrêter l'exécution de la requête spécifiée	Écrire	workgroup*		
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource	Identification	capacity-reservation*		
			datacatalog*		
			session*		
			workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateSession	Accorde l'autorisation de mettre fin à une session	Écrire	workgroup*		
			session		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	capacity-reservation*		
			datacatalog*		
			session*		
			workgroup*		
				aws:TagKeys	
UpdateCapacityReservation	Accorde l'autorisation de mettre à jour une réservation de capacité	Écrire	capacity-reservation*		
UpdateDataCatalog	Accorde l'autorisation nécessaire pour mettre à jour un catalogue de données	Écrire	datacatalog*		
UpdateNamedQuery	Accorde l'autorisation nécessaire pour mettre à jour une requête nommée spécifiée	Écrire	workgroup*		
UpdateNotebook	Accorde l'autorisation de mettre à jour un bloc-notes	Écrire	workgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNotebookMetadata	Accorde l'autorisation de mettre à jour les métadonnées du bloc-notes	Écrire	workgroup *		
UpdatePreparedStatement	Accorde l'autorisation nécessaire pour mettre à jour une déclaration préparée	Écrire	workgroup *		
UpdateWorkGroup	Accorde l'autorisation nécessaire pour mettre à jour un groupe de travail	Écrire	workgroup *		

Types de ressources définis par Amazon Athena

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
datacatalog	`arn:${Partition}:athena:${Region}:${Account}:datacatalog/${DataCatalogName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
capacity-reservation	`arn:${Partition}:athena:${Region}:${Account}:capacity-reservation/${CapacityReservationName}`	aws:ResourceTag/${TagKey}
session	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}/session/${SessionId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Athena

Amazon Athena définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la requête	ArrayOfString

Actions, ressources et clés de condition pour AWS Audit Manager

AWS Audit Manager (préfixe de service :`auditmanager`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l' AWS Audit Manager
- Types de ressources définis par AWS Audit Manager
- Clés de condition pour AWS Audit Manager

Actions définies par l' AWS Audit Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAssessmentReportEvidenceFolder	Autorise l'association d'un dossier de preuves à un rapport d'évaluation dans AWS Audit Manager	Écrire	assessment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchAssociateAssessmentReportEvidence	Autorise l'association d'une liste de preuves à un rapport d'évaluation dans AWS Audit Manager	Écrire	assessment*		
BatchCreateDelegationByAssessment	Autorise la création de délégations pour une évaluation dans AWS Audit Manager	Écrire	assessment*		
			assessmentControlSet*		
BatchDeleteDelegationByAssessment	Accorde l'autorisation de supprimer des délégations pour une évaluation dans AWS Audit Manager	Écrire	assessment*		
			assessmentControlSet*		
BatchDisassociateAssessmentReportEvidence	Autorise à dissocier une liste de preuves d'un rapport d'évaluation dans AWS Audit Manager	Écrire	assessment*		
BatchImportEvidenceToAssessmentControl	Autorise l'importation d'une liste de preuves dans un contrôle d'évaluation dans AWS Audit Manager	Écrire	assessmentControlSet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAssessment	Accorde l'autorisation de créer une évaluation à utiliser avec AWS Audit Manager	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentFramework	Accorde l'autorisation de créer un framework à utiliser dans AWS Audit Manager	Écrire	assessmentFramework*		
			control*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentReport	Autorise la création d'un rapport d'évaluation dans AWS Audit Manager	Écrire	assessment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateControl	Accorde l'autorisation de créer un contrôle à utiliser dans AWS Audit Manager	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAssessment	Autorise la suppression d'une évaluation dans AWS Audit Manager	Écrire	assessment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFramework	Autorise la suppression d'un cadre d'évaluation dans AWS Audit Manager	Écrire	assessmentFramework*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAssessmentFrameworkShare	Accorde l'autorisation de supprimer une demande de partage pour un framework personnalisé dans AWS Audit Manager	Écrire			
DeleteAssessmentReport	Autorise la suppression d'un rapport d'évaluation dans AWS Audit Manager	Écrire	assessment*		
DeleteControl	Accorde l'autorisation de supprimer un contrôle dans AWS Audit Manager	Écrire	control*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeregisterAccount	Accorde l'autorisation de désenregistrer un compte dans Audit Manager AWS	Écrire			
DeregisterOrganizationAdminAccount	Accorde l'autorisation de désenregistrer le compte d'administrateur délégué pour Audit Manager AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateAssessmentReportEvidenceFolder	Autorise à dissocier un dossier de preuves d'un rapport d'évaluation dans AWS Audit Manager	Écrire	assessment*		
GetAccountStatus	Accorde l'autorisation d'obtenir le statut d'un compte dans AWS Audit Manager	Lecture			
GetAssessment	Accorde l'autorisation de créer une évaluation dans AWS Audit Manager	Lecture	assessment*		
GetAssessmentFramework	Accorde l'autorisation d'obtenir un cadre d'évaluation dans AWS Audit Manager	Lecture	assessmentFramework*		
GetAssessmentReportUrl	Accorde l'autorisation d'obtenir l'URL d'un rapport d'évaluation dans AWS Audit Manager	Lecture	assessment*		
GetChangeLogs	Accorde l'autorisation d'obtenir les journaux des modifications pour une évaluation dans Audit Manager AWS	Lecture	assessment*		
GetControl	Accorde l'autorisation d'obtenir un contrôle dans AWS Audit Manager	Lecture	control*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDelegations	Accorde l'autorisation d'obtenir toutes les délégations dans AWS Audit Manager	List			
GetEvidence	Donne l'autorisation d'obtenir des preuves auprès de l' AWS Audit Manager	Lecture	assessmentControlSet*		
GetEvidenceByEvidenceFolder	Accorde l'autorisation d'obtenir toutes les preuves d'un dossier de preuves dans AWS Audit Manager	Lecture	assessmentControlSet*		
GetEvidenceFileUploadUrl	Accorde l'autorisation d'obtenir une URL Amazon S3 présignée qui peut être utilisée pour télécharger un fichier en tant que preuve manuelle	Lecture			
GetEvidenceFolder	Accorde l'autorisation d'obtenir le dossier de preuves auprès d' AWS Audit Manager	Lecture	assessmentControlSet*		
GetEvidenceFoldersByAssessment	Accorde l'autorisation d'obtenir les dossiers de preuves d'une évaluation dans AWS Audit Manager	Lecture	assessment*		
GetEvidenceFoldersByAssessmentControl	Accorde l'autorisation d'obtenir les dossiers de preuves à partir d'un contrôle d'évaluation dans AWS Audit Manager	Lecture	assessmentControlSet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInsights	Accorde l'autorisation d'obtenir des données analytiques pour toutes les évaluations actives	Lecture			
GetInsightsByAssessment	Accorde l'autorisation d'obtenir des données analytiques pour une évaluation active spécifique	Lecture			
GetOrganizationAdminAccount	Accorde l'autorisation d'obtenir le compte d'administrateur délégué dans AWS Audit Manager	Lecture			
GetServicesInScope	Accorde l'autorisation d'inclure les services dans le cadre d'une évaluation dans AWS Audit Manager	Lecture			
GetSettings	Accorde l'autorisation de configurer tous les paramètres dans AWS Audit Manager	Lecture			
ListAssessmentControlInsightsByControlDomain	Accorde l'autorisation de répertorier les données analytiques pour les contrôles dans un domaine de contrôle spécifique et une évaluation active	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAssessmentFrameworkShareRequests	Accorde l'autorisation de répertorier toutes les demandes de partage envoyées ou reçues pour des frameworks personnalisés dans AWS Audit Manager	List			
ListAssessmentFrameworks	Permet de répertorier tous les cadres d'évaluation dans AWS Audit Manager	List			
ListAssessmentReports	Autorise à répertorier tous les rapports d'évaluation dans AWS Audit Manager	List			
ListAssessments	Autorise à répertorier toutes les évaluations dans AWS Audit Manager	List			
ListControlDomainInsights	Accorde l'autorisation de répertorier les données analytiques pour les domaines de contrôle dans toutes les évaluations actives	List			
ListControlDomainInsightsByAssessment	Accorde l'autorisation de répertorier les données analytiques pour les domaines de contrôle dans une évaluation active spécifique	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListControlInsightsByControlDomain	Accorde l'autorisation de répertorier les données analytiques pour les contrôles d'un domaine de contrôle spécifique pour toutes les évaluations actives	List			
ListControls	Accorde l'autorisation de répertorier tous les contrôles dans AWS Audit Manager	List			
ListKeywordsForDataSource	Accorde l'autorisation de répertorier tous les mots clés des sources de données dans AWS Audit Manager	List			
ListNotifications	Accorde l'autorisation de répertorier toutes les notifications dans AWS Audit Manager	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource AWS Audit Manager	Lecture	assessment control		
RegisterAccount	Autorise l'enregistrement d'un compte dans AWS Audit Manager	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterOrganizationAdminAccount	Accorde l'autorisation d'enregistrer un compte au sein de l'organisation en tant qu'administrateur délégué d' AWS Audit Manager	Écrire			
StartAssessmentFrameworkShare	Accorde l'autorisation de créer une demande de partage pour un framework personnalisé dans AWS Audit Manager	Écrire	assessmentFramework*		
TagResource	Accorde l'autorisation de baliser une ressource AWS Audit Manager	Identification	assessment		
			assessmentFramework		
			control		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource AWS Audit Manager	Identification	assessment	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			assessmentFramework	aws:ResourceTag/${TagKey}	
			control	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateAssessment	Autorise la mise à jour d'une évaluation dans AWS Audit Manager	Écrire	assessment*		
UpdateAssessmentControl	Autorise la mise à jour d'un contrôle d'évaluation dans AWS Audit Manager	Écrire	assessmentControlSet*		
UpdateAssessmentControlSetStatus	Autorise la mise à jour du statut d'un ensemble de contrôles d'évaluation dans AWS Audit Manager	Écrire	assessmentControlSet*		
UpdateAssessmentFramework	Autorise la mise à jour d'un cadre d'évaluation dans AWS Audit Manager	Écrire	assessmentFramework*		
			control*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAssessmentFrameworkShare	Accorde l'autorisation de mettre à jour une demande de partage pour un framework personnalisé dans AWS Audit Manager	Écrire	assessmentFramework*		
UpdateAssessmentStatus	Autorise la mise à jour du statut d'une évaluation dans AWS Audit Manager	Écrire	assessment*		
UpdateControl	Autorise la mise à jour d'un contrôle dans AWS Audit Manager	Écrire	control*		
UpdateSettings	Autorise la mise à jour des paramètres dans AWS Audit Manager	Écrire			
ValidateAssessmentReportIntegrity	Autorise à valider l'intégrité d'un rapport d'évaluation dans AWS Audit Manager	Lecture			

Types de ressources définis par AWS Audit Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
assessment	arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}	aws:ResourceTag/${TagKey}
assessmentFramework	arn:${Partition}:auditmanager:${Region}:${Account}:assessmentFramework/${AssessmentFrameworkId}	aws:ResourceTag/${TagKey}
assessmentControlSet	arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}/controlSet/${ControlSetId}	
control	arn:${Partition}:auditmanager:${Region}:${Account}:control/${ControlId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Audit Manager

AWS Audit Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Aurora DSQL

Amazon Aurora DSQL (préfixe de service :`dsql`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Aurora DSQL
- Types de ressources définis par Amazon Aurora DSQL
- Clés de condition pour Amazon Aurora DSQL

Actions définies par Amazon Aurora DSQL

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddPeerCluster [autorisation uniquement]	Accorde l'autorisation d'ajouter un cluster homologue à un cluster multirégional	Écrire	Cluster*		dsql:PutMultiRegionProperties
CreateCluster	Accorde l'autorisation de créer de nouveaux clusters	Écrire	Cluster*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys dsql:WitnessRegion	
DbConnect	Accorde l'autorisation de se connecter à la base de données	Écrire	Cluster*		
DbConnectAdmin	Accorde l'autorisation de se connecter à la base de données avec le rôle d'administrateur. La connexion à un autre rôle nécessite une DbConnect autorisation	Écrire	Cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCluster	Autorise la suppression d'un cluster et de toutes ses données	Écrire	Cluster*		
DeleteClusterPolicy	Accorde l'autorisation de supprimer la politique intégrée basée sur les ressources attachée à un cluster	Écrire	Cluster*		
GetBackupJob	Accorde l'autorisation d'obtenir le statut d'une tâche de sauvegarde d'un cluster Aurora DSQL	Lecture	Cluster*		
GetCluster	Accorde l'autorisation d'obtenir des informations sur un cluster	Lecture	Cluster*		
GetClusterPolicy	Accorde l'autorisation de récupérer la politique intégrée basée sur les ressources attachée à un cluster	Lecture	Cluster*		
GetRestoreJob	Accorde l'autorisation d'obtenir l'état d'une tâche de restauration d'un cluster Aurora DSQL	Lecture	Cluster*		
GetVpcEndpointServiceName	Accorde l'autorisation de récupérer le nom du service de point de terminaison VPC pour un cluster	Lecture	Cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InjectError [autorisation uniquement]	Accorde l'autorisation d'injecter des erreurs dans les clusters ciblés	Écrire		dsql:FisActionId dsql:FisTargetArns	
ListClusters	Accorde l'autorisation de récupérer une liste de clusters	List			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises d'une ressource SQL Aurora	Lecture	Cluster*		
PutClusterPolicy	Accorde l'autorisation d'associer ou de mettre à jour la politique intégrée basée sur les ressources attachée à un cluster	Écrire	Cluster*		
PutMultiRegionProperties [autorisation uniquement]	Autorise la mise à jour des propriétés multirégionales d'un cluster	Écrire	Cluster*		
PutWitnessRegion [autorisation uniquement]	Accorde l'autorisation de configurer et de mettre à jour la région témoin d'un cluster multirégional	Écrire	Cluster*		dsql:PutMultiRegionProperties
				dsql:WitnessRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemovePeerCluster [autorisation uniquement]	Accorde l'autorisation de supprimer un cluster homologue d'un cluster multirégional	Écrire	Cluster*		dsql:PutMultiRegionProperties
StartBackupJob	Accorde l'autorisation de démarrer une tâche de sauvegarde pour un cluster SQL Aurora	Écrire	Cluster*		
StartRestoreJob	Accorde l'autorisation de démarrer une tâche de restauration pour un cluster Aurora DSQL	Écrire	Cluster*		dsql:CreateCluster iam:CreateServiceLinkedRole
StopBackupJob	Autorise l'arrêt d'une tâche de sauvegarde pour un cluster Aurora DSQL	Écrire	Cluster*		
StopRestoreJob	Autorise l'arrêt d'une tâche de restauration pour un cluster Aurora DSQL	Écrire	Cluster*		
TagResource	Accorde l'autorisation d'ajouter des balises aux ressources SQL Aurora	Identification	Cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des balises des ressources SQL Aurora	Identification	Cluster*		
				aws:TagKeys	
UpdateCluster	Accorde l'autorisation de modifier les attributs du cluster	Écrire	Cluster*		
				dsql:WitnessRegion	

Types de ressources définis par Amazon Aurora DSQL

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Cluster	`arn:${Partition}:dsql:${Region}:${Account}:cluster/${Identifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Aurora DSQL

Amazon Aurora DSQL définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
dsql:FisActionId	Filtre l'accès en fonction de l'ID d'une AWS action FIS	String
dsql:FisTargetArns	Filtre l'accès par l'ARN d'une AWS cible FIS	ArrayOfARN
dsql:WitnessRegion	Filtre l'accès par région témoin des clusters multirégionaux	String

Actions, ressources et clés de condition pour AWS Auto Scaling

AWS Auto Scaling (préfixe de service :`autoscaling-plans`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Auto Scaling

- Types de ressources définis par AWS Auto Scaling
- Clés de condition pour AWS Auto Scaling

Actions définies par AWS Auto Scaling

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateScalingPlan	Crée un plan de mise à l'échelle.	Écriture			
DeleteScalingPlan	Supprime le plan de dimemise à l'échelle spécifié.	Écriture			
DescribeScalingPlanResources	Décrit les ressources évolutives du plan de dimmise à l'échelle spécifié.	Lecture			
DescribeScalingPlans	Décrit les plans de mise à l'échelle spécifiés ou tous vos plans de mise à l'échelle.	Lecture			
GetScalingPlanResourceForecastData	Récupère les données prévisionnelles d'une ressource évolutive.	Lecture			
UpdateScalingPlan	Met à jour un plan de mise à l'échelle.	Écrire			

Types de ressources définis par AWS Auto Scaling

AWS Auto Scaling ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Auto Scaling, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Auto Scaling

Auto Scaling ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour l'échange de données AWS B2B

AWS L'échange de données B2B (préfixe de service :`b2bi`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'échange AWS de données B2B
- Types de ressources définis par AWS B2B Data Interchange
- Clés de condition pour l' AWS échange de données B2B

Actions définies par l'échange AWS de données B2B

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCapability	Octroie l'autorisation de créer une capacité.	Écrire	transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePartnership	Octroie l'autorisation de créer un partenariat.	Écrire	capability*		
			profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile	Accorde l'autorisation de créer un profil	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateStarterMappingTemplate	Accorde l'autorisation de générer un JSONATA/XSLT modèle de démarrage	Écrire	transformer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTransformer	Octroie l'autorisation de créer un transformateur.	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCapability	Octroie l'autorisation de supprimer une capacité.	Écrire	capability*		
DeletePartnership	Octroie l'autorisation de supprimer un partenariat.	Écrire	partnership*		
DeleteProfile	Accorde l'autorisation de supprimer un profil.	Écrire	profile*		
DeleteTransformer	Octroie l'autorisation de supprimer un transformateur.	Écrire	transformer*		
GenerateMapping	Autorise la génération d'un modèle de JSONATA/XSLT cartographie de démarrage à partir d'Amazon Bedrock	Écrire	transformer*		
GetCapability	Octroie l'autorisation d'obtenir une capacité.	Lecture	capability*		
GetPartnership	Octroie l'autorisation d'obtenir un partenariat.	Lecture	partnership*		
GetProfile	Accorde l'autorisation d'obtenir un profil	Lecture	profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTransformer	Octroie l'autorisation d'obtenir un transformateur.	Lecture	transformer*		
GetTransformerJob	Octroie l'autorisation d'obtenir une tâche de transformateur.	Lecture	transformer*		
ListCapabilities	Octroie l'autorisation de répertorier toutes les capacités .	List			
ListPartnerships	Octroie l'autorisation de répertorier tous les partenariats.	List			
ListProfiles	Octroie l'autorisation de répertorier tous les profils.	List			
ListTagsForResource	Octroie l'autorisation de répertorier les balises d'une ressource B2Bi.	Lecture	capability		
			partnership		
			profile		
			transformer		
ListTransformers	Octroie l'autorisation de répertorier tous les transformateurs.	List			
StartTransformerJob	Octroie l'autorisation de transformer un document.	Écrire	transformer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Octroie l'autorisation de baliser une ressource B2Bi.	Identification	capability		
			partnership		
			profile		
			transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConversion	Accorde l'autorisation de JSON/XML convertir un document en document EDI	Écrire	transformer*		
TestMapping	Octroie l'autorisation de mapper un fichier d'exemple.	Écrire	transformer*		
TestParsing	Octroie l'autorisation d'analyser un document EDI.	Écrire	transformer*		
UntagResource	Octroie l'autorisation d'annuler le balisage d'une ressource B2Bi.	Identification	capability		
			partnership		
			profile		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			transformer		
				aws:TagKeys	
UpdateCapability	Octroie l'autorisation de mettre à jour une capacité.	Écrire	capability*		
			transformer		
UpdatePartnership	Octroie l'autorisation de mettre à jour un partenariat.	Écrire	partnership*		
			capability		
UpdateProfile	Accorde l'autorisation de mettre à jour un profil	Écrire	profile*		
UpdateTransformer	Octroie l'autorisation de mettre à jour un transformateur.	Écrire	transformer*		

Types de ressources définis par AWS B2B Data Interchange

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
profile	arn:${Partition}:b2bi:${Region}:${Account}:profile/${ResourceId}	aws:ResourceTag/${TagKey}
capability	arn:${Partition}:b2bi:${Region}:${Account}:capability/${ResourceId}	aws:ResourceTag/${TagKey}
partnership	arn:${Partition}:b2bi:${Region}:${Account}:partnership/${ResourceId}	aws:ResourceTag/${TagKey}
transformer	arn:${Partition}:b2bi:${Region}:${Account}:transformer/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour l' AWS échange de données B2B

AWS L'échange de données B2B définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Backup

AWS Backup (préfixe de service :`backup`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Backup
- Types de ressources définis par AWS Backup
- Clés de condition pour AWS Backup

Actions définies par AWS Backup

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateBackupVaultMpaApprovalTeam	Accorde l'autorisation d'associer une équipe d'approbation MPA à un coffre-fort de sauvegarde	Écrire	backupVault*		
				backup:MpaApprovalTeamArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelLegalHold	Accorde l'autorisation d'annuler une mise en suspens juridique	Écrire	legalHold*		
CopyFromBackupVault [autorisation uniquement]	Accorde l'autorisation d'effectuer une copie à partir d'un coffre de sauvegarde	Écriture	recoveryPoint*		
				backup:CopyTargets backup:CopyTargetOrgPaths	
CopyIntoBackupVault [autorisation uniquement]	Accorde l'autorisation d'effectuer une copie dans un coffre de sauvegarde	Écrire	backupVault*		
				aws:RequestTag/${TagKey}	
CreateBackupAccessPoint [autorisation uniquement]	Autorise la création d'un nouveau point d'accès pour un accès instantané aux sauvegardes	Écrire	recoveryPoint*		
CreateBackupPlan	Accorde l'autorisation de créer un plan de sauvegarde	Écriture	backupPlan*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackupSelection	Accorde l'autorisation de créer une attribution de ressource dans un plan de sauvegarde	Écriture	backupPlan*		iam:PassRole
CreateBackupVault	Accorde l'autorisation de créer un coffre de sauvegarde	Écrire	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFramework	Accorde l'autorisation de créer un cadre	Écrire	framework*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLegalHold	Accorde l'autorisation de créer une nouvelle mise en suspens juridique	Écrire	legalHold*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogicallyAirGappedBackupVault	Accorde l'autorisation de créer un nouveau coffre-fort de sauvegarde logiquement cloisonné, un conteneur logique dans lequel les sauvegardes sont stockées	Écrire	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:MinRetentionDays backup:MaxRetentionDays	
CreateReportPlan	Accorde l'autorisation de créer un plan de rapport	Écrire	reportPlan*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys backup:FrameworkArns	
CreateRestoreAccessBackupVault	Autorise la création d'un coffre-fort de sauvegarde pour l'accès à la restauration	Écrire	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingPlan	Octroie l'autorisation de créer un plan de test de la restauration.	Écrire	restoreTestingPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRestoreTestingSelection	Octroie l'autorisation de créer une attribution de ressource dans un plan de test de la restauration.	Écrire	restoreTestingPlan*		iam:PassRole
CreateTieringConfiguration	Accorde l'autorisation de créer une nouvelle configuration de hiérarchisation	Écrire	tieringConfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBackupAccessPoint [autorisation uniquement]	Accorde l'autorisation de supprimer le point d'accès	Écrire			
DeleteBackupPlan	Accorde l'autorisation de supprimer un plan de sauvegarde	Écriture	backupPlan*		
DeleteBackupSelection	Accorde l'autorisation de supprimer une attribution de ressource dans un plan de sauvegarde	Écriture	backupPlan*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBackupVault	Accorde l'autorisation de supprimer un coffre de sauvegarde	Écriture	backupVault*		
DeleteBackupVaultAccessPolicy	Accorde l'autorisation de supprimer une politique d'accès à un coffre de sauvegarde	Gestion des autorisations	backupVault*		
DeleteBackupVaultLockConfiguration	Accorde l'autorisation de supprimer la configuration de verrouillage d'un coffre de sauvegarde	Écrire	backupVault*		
DeleteBackupVaultNotifications	Accorde l'autorisation de supprimer les notifications d'un coffre de sauvegarde	Écrire	backupVault*		
DeleteBackupVaultSharingPolicy [autorisation uniquement]	Octroie l'autorisation de supprimer une stratégie de partage d'un coffre-fort de sauvegarde.	Gestion des autorisations	backupVault*		
DeleteFramework	Accorde l'autorisation de supprimer un cadre	Écrire	framework*		
DeleteRecoveryPoint	Accorde l'autorisation de supprimer un point de récupération dans un coffre de sauvegarde	Écrire	recoveryPoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteReportPlan	Accorde l'autorisation de supprimer un plan de rapport	Écrire	reportPlan*		
DeleteRestoreTestingPlan	Octroie l'autorisation de supprimer un plan de test de la restauration.	Écrire	restoreTestingPlan*		
DeleteRestoreTestingSelection	Octroie l'autorisation de supprimer une attribution de ressource d'un plan de test de la restauration.	Écrire	restoreTestingPlan*		
DeleteTieringConfiguration	Accorde l'autorisation de supprimer une configuration de hiérarchisation	Écrire	tieringConfiguration*		
DescribeBackupAccessPoint [autorisation uniquement]	Accorde l'autorisation de renvoyer des informations sur le point d'accès spécifié	Lecture			
DescribeBackupJob	Accorde l'autorisation de décrire une tâche de sauvegarde	Lecture			
DescribeBackupVault	Accorde l'autorisation de décrire un nouveau coffre de sauvegarde avec le nom spécifié	Lecture	backupVault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCopyJob	Accorde l'autorisation de décrire une tâche de copie	Lecture			
DescribeFramework	Accorde l'autorisation de décrire un cadre avec le nom spécifié	Lecture	framework*		
DescribeGlobalSettings	Accorde l'autorisation de décrire des paramètres globaux	Lecture			
DescribeProtectedResource	Accorde l'autorisation de décrire une ressource protégée	Lecture			
DescribeRecoveryPoint	Accorde l'autorisation de décrire un point de récupération	Lecture	recoveryPoint*		
DescribeRegionSettings	Accorde l'autorisation de décrire des paramètres de région	Lecture			
DescribeReportJob	Accorde l'autorisation de décrire une tâche de rapport	Lecture			
DescribeReportPlan	Accorde l'autorisation de décrire un plan de rapport avec le nom spécifié	Lecture	reportPlan*		
DescribeRestoreJob	Accorde l'autorisation de décrire une tâche de restauration	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeScanJob	Accorde l'autorisation de décrire une tâche de numérisation	Lecture			
DisassociateBackupVaultMpaApprovalTeam	Accorde l'autorisation de dissocier une équipe d'approbation MPA d'un coffre-fort de sauvegarde	Écrire	backupVault*		
DisassociateRecoveryPoint	Accorde l'autorisation de dissocier un point de récupération d'un coffre de sauvegarde	Écrire	recoveryPoint*		
DisassociateRecoveryPointFromParent	Accorde l'autorisation de dissocier un point de récupération de son parent	Écrire	recoveryPoint*		
ExportBackupPlanTemplate	Accorde l'autorisation d'exporter un plan de sauvegarde au format JSON	Lecture			
GetBackupPlan	Accorde l'autorisation d'obtenir un plan de sauvegarde	Lecture	backupPlan*		
GetBackupPlanFromJSON	Accorde l'autorisation de transformer un fichier JSON en plan de sauvegarde	Lecture			
GetBackupPlanFromTemplate	Accorde l'autorisation de transformer un modèle en plan de sauvegarde	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBackupSelection	Accorde l'autorisation d'obtenir une attribution de ressource de plan de sauvegarde	Lecture	backupPlan*		
GetBackupVaultAccessPolicy	Accorde l'autorisation d'obtenir la politique d'accès au coffre de sauvegarde	Lecture	backupVault*		
GetBackupVaultNotifications	Accorde l'autorisation d'obtenir les notifications du coffre de sauvegarde	Lecture	backupVault*		
GetBackupVaultSharingPolicy [autorisation uniquement]	Octroie l'autorisation d'obtenir une stratégie de partage d'un coffre-fort de sauvegarde.	Lecture	backupVault*		
GetLegalHold	Accorde l'autorisation d'obtenir une mise en suspens juridique	Lecture	legalHold*		
GetRecoveryPointIndexDetails	Accorde l'autorisation d'obtenir les détails d'indexation d'un point de récupération	Lecture	recoveryPoint*		
GetRecoveryPointRestoreMetadata	Accorde l'autorisation d'obtenir les métadonnées de restauration du point de récupération	Lecture	recoveryPoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRestoreJobMetadata	Octroie l'autorisation d'obtenir les métadonnées de restauration associées à une tâche de restauration.	Lecture			
GetRestoreTestingInferredMetadata	Octroie l'autorisation d'obtenir les métadonnées déduites générées par les tests de restauration.	Lecture			
GetRestoreTestingPlan	Octroie l'autorisation d'obtenir un plan de test de la restauration.	Lecture	restoreTestingPlan*		
GetRestoreTestingSelection	Octroie l'autorisation d'obtenir une attribution de ressource pour un plan de test de la restauration.	Lecture	restoreTestingPlan*		
GetSupportedResourceTypes	Accorde l'autorisation d'obtenir les types de ressources pris en charge	Lecture			
GetTieringConfiguration	Accorde l'autorisation de décrire une configuration de hiérarchisation	Lecture	tieringConfiguration*		
ListBackupJobSummaries	Accorde l'autorisation de répertorier les récapitulatifs des tâches de sauvegarde	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBackupJobs	Accorde l'autorisation de répertorier les tâches de sauvegarde	List			
ListBackupPlanTemplates	Autorise à répertorier les modèles de plan de sauvegarde fournis par AWS Backup	List			
ListBackupPlanVersions	Accorde l'autorisation de répertorier les versions des plans de sauvegarde	List	backupPlan*		
ListBackupPlans	Accorde l'autorisation de répertorier les plans de sauvegarde	List			
ListBackupSelections	Accorde l'autorisation de répertorier des attributions de ressources d'un plan de sauvegarde spécifique	List	backupPlan*		
ListBackupVaults	Accorde l'autorisation de répertorier les coffres de sauvegarde	List			
ListCopyJobSummaries	Accorde l'autorisation de répertorier les récapitulatifs des tâches de copie	List			
ListCopyJobs	Accorde l'autorisation de répertorier les tâches de copie.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFrameworks	Autorise l'autorisation de répertorier les cadres	List			
ListIndexedRecoveryPoints	Autorise l'accès à la liste des points de récupération indexés	List			
ListIndexedRecoveryPointsForSearch [autorisation uniquement]	Permet de répertorier les points de récupération indexés à rechercher	Gestion des autorisations			
ListLegalHolds	Accorde l'autorisation de répertorier des mises en suspens juridiques	List			
ListProtectedResources	Accorde l'autorisation de répertorier les ressources protégées par AWS Backup	List			
ListProtectedResourcesByBackupVault	Octroie l'autorisation de répertorier les ressources protégées d'un coffre-fort de sauvegarde.	List	backupVault*		
ListRecoveryPointsByBackupVault	Accorde l'autorisation de répertorier les points de récupération dans un coffre de sauvegarde	List	backupVault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRecoveryPointsByLegalHold	Accorde l'autorisation de répertorier les points de récupération en fonction d'une mise en suspens juridique	List	legalHold*		
ListRecoveryPointsByResource	Accorde l'autorisation de répertorier les points de récupération d'une ressource	List			
ListReportJobs	Accorde l'autorisation de répertorier les tâches de rapport	List			
ListReportPlans	Accorde l'autorisation de répertorier les plans de rapport	List			
ListRestoreAccessBackupVaults	Accorde l'autorisation de répertorier un coffre-fort de sauvegarde avec accès à la restauration associé à un coffre-fort de sauvegarde	List	backupVault*		
ListRestoreJobSummaries	Accorde l'autorisation de répertorier les récapitulatifs des tâches	List			
ListRestoreJobs	Octroie l'autorisation de répertorier les tâches de restauration.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRestoreJobsByProtectedResource	Octroie l'autorisation de répertorier les tâches de restauration pour une ressource protégée.	List			
ListRestoreTestingPlans	Octroie l'autorisation de répertorier les plans de test de la restauration.	List			
ListRestoreTestingSelections	Octroie l'autorisation de répertorier des attributions de ressources d'un plan de test de la restauration spécifique.	List	restoreTestingPlan *		
ListScanJobSummaries	Accorde l'autorisation de répertorier les résumés des tâches de numérisation	List			
ListScanJobs	Accorde l'autorisation de répertorier les tâches de numérisation	List			
ListTags	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	backupPlan		
			backupVault		
			framework		
			legalHold		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
			tieringConfiguration		
ListTieringConfigurations	Accorde l'autorisation de répertorier les configurations de hiérarchisation	List			
PutBackupVaultAccessPolicy	Accorde l'autorisation d'ajouter une politique d'accès au coffre de sauvegarde	Gestion des autorisations	backupVault*		
PutBackupVaultLockConfiguration	Accorde l'autorisation d'ajouter une configuration de verrouillage à un coffre de sauvegarde	Écrire	backupVault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				backup:ChangeableForDays backup:MinRetentionDays backup:MaxRetentionDays	
PutBackupVaultNotifications	Accorde l'autorisation d'ajouter une rubrique SNS au coffre de sauvegarde	Écrire	backupVault*		
PutBackupVaultSharingPolicy [autorisation uniquement]	Octroie l'autorisation d'ajouter une stratégie de partage au coffre-fort de sauvegarde.	Gestion des autorisations	backupVault*		
PutRestoreValidationResult	Octroie l'autorisation de saisir un résultat de validation de restauration.	Écrire			
RevokeRestoreAccessBackupVault	Autorise la révocation d'un coffre de sauvegarde d'accès à la restauration	Écrire	backupVault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchRecoveryPoint [autorisation uniquement]	Autorise la recherche d'un point de récupération	Gestion des autorisations	recoveryPoint*		
StartBackupJob	Accorde l'autorisation de démarrer une nouvelle tâche de sauvegarde	Écriture	backupVault*		iam:PassRole
StartCopyJob	Accorde l'autorisation de copier une sauvegarde entre un coffre de sauvegarde source et un coffre de sauvegarde de destination	Écrire	recoveryPoint*		iam:PassRole
StartReportJob	Accorde l'autorisation de démarrer une nouvelle tâche de rapport	Écrire	reportPlan*		
StartRestoreJob	Accorde l'autorisation de démarrer une nouvelle tâche de restauration	Écrire	recoveryPoint*		iam:PassRole
StartScanJob	Accorde l'autorisation de démarrer une nouvelle tâche de numérisation	Écrire	recoveryPoint*		iam:PassRole
StopBackupJob	Accorde l'autorisation d'arrêter une tâche de sauvegarde	Écriture			
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	backupPlan		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
			tieringConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	backupPlan		
			backupVault		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
			tieringConfiguration		
				aws:TagKeys	
UpdateBackupPlan	Accorde l'autorisation de mettre à jour un plan de sauvegarde	Écrire	backupPlan*		iam:PassRole
UpdateFramework	Accorde l'autorisation de mettre à jour un cadre	Écrire	framework*		
UpdateGlobalSettings	Autorise la mise à jour des paramètres globaux actuels du AWS compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRecoveryPointIndexSettings	Autorise la mise à jour des paramètres de l'index des points de récupération	Écrire	recoveryPoint*		
				backup:Index	
UpdateRecoveryPointLifecycle	Accorde l'autorisation de mettre à jour le cycle de vie du point de récupération	Écriture	recoveryPoint*		
UpdateRegionSettings	Accorde l'autorisation de mettre à jour les paramètres actuels d'acceptation du service pour la région	Écrire			
UpdateReportPlan	Accorde l'autorisation de mettre à jour un plan de rapport	Écrire	reportPlan*		
				backup:FrameworkArns	
UpdateRestoreTestingPlan	Octroie l'autorisation de mettre à jour un plan de test de la restauration.	Écrire	restoreTestingPlan*		
UpdateRestoreTestingSelection	Octroie l'autorisation de mettre à jour une attribution de ressource dans un plan de test de la restauration.	Écrire	restoreTestingPlan*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTieringConfiguration	Accorde l'autorisation de mettre à jour une configuration de hiérarchisation	Écrire	tieringConfiguration*		

Types de ressources définis par AWS Backup

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
backupVault	`arn:${Partition}:backup:${Region}:${Account}:backup-vault:${BackupVaultName}`	aws:ResourceTag/${TagKey}
backupPlan	`arn:${Partition}:backup:${Region}:${Account}:backup-plan:${BackupPlanId}`	aws:ResourceTag/${TagKey}
recoveryPoint	`arn:${Partition}:${Vendor}:${Region}:*:${ResourceType}:${RecoveryPointId}`	aws:ResourceTag/${TagKey}
framework	`arn:${Partition}:backup:${Region}:${Account}:framework:${FrameworkName}-${FrameworkId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
reportPlan	arn:${Partition}:backup:${Region}:${Account}:report-plan:${ReportPlanName}-${ReportPlanId}	aws:ResourceTag/${TagKey}
legalHold	arn:${Partition}:backup:${Region}:${Account}:legal-hold:${LegalHoldId}	aws:ResourceTag/${TagKey}
restoreTestingPlan	arn:${Partition}:backup:${Region}:${Account}:restore-testing-plan:${RestoreTestingPlanName}-${RestoreTestingPlanId}	aws:ResourceTag/${TagKey}
tieringConfiguration	arn:${Partition}:backup:${Region}:${Account}:tiering-configuration:${TieringConfigurationName}-${TieringConfigurationId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Backup

AWS Backup définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString
backup:ChangeableForDays	Filtre l'accès en fonction de la valeur du ChangeableForDays paramètre	Numérique
backup:CopyTargetOrgPaths	Filtre l'accès en fonction de l'unité d'organisation	ArrayOfString
backup:CopyTargets	Filtre l'accès par l'ARN d'un coffre de sauvegarde	ArrayOfARN
backup:FrameworkArns	Filtre l'accès par le Framework ARNs	ArrayOfARN
backup:Index	Filtre l'accès en fonction de la valeur du paramètre Index	String
backup:MaxRetentionDays	Filtre l'accès en fonction de la valeur du MaxRetentionDays paramètre	Numérique
backup:MinRetentionDays	Filtre l'accès en fonction de la valeur du MinRetentionDays paramètre	Numérique
backup:MpaApprovalTeamArn	Filtre l'accès par l'équipe d'approbation MPA (ARN) d'un coffre-fort de sauvegarde	ARN

Actions, ressources et clés de condition pour AWS Backup Gateway

AWS Backup Gateway (préfixe de service :`backup-gateway`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Backup Gateway
- Types de ressources définis par AWS Backup Gateway
- Clés de condition pour AWS Backup Gateway

Actions définies par AWS Backup Gateway

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateGatewayToServer	Accorde l'autorisation à AssociateGatewayToServer	Écrire	gateway*		
			hypervisor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Backup	Accorde l'autorisation à Backup	Écrire	virtualmachine*		
CreateGateway	Accorde l'autorisation de CreateGateway	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGateway	Accorde l'autorisation à DeleteGateway	Écrire	gateway*		
DeleteHypervisor	Accorde l'autorisation à DeleteHypervisor	Écrire	hypervisor*		
DisassociateGatewayFromServer	Accorde l'autorisation à DisassociateGatewayFromServer	Écrire	gateway*		
GetBandwidthRateLimitSchedule	Accorde l'autorisation à GetBandwidthRateLimitSchedule	Lecture	gateway*		
GetGateway	Accorde l'autorisation à GetGateway	Lecture	gateway*		
GetHypervisor	Accorde l'autorisation à GetHypervisor	Lecture	hypervisor*		
GetHypervisorPropertyMappings	Accorde l'autorisation à GetHypervisorPropertyMappings	Lecture	hypervisor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetVirtualMachine	Accorde l'autorisation à GetVirtualMachine	Lecture	virtualmachine*		
ImportHypervisorConfiguration	Accorde l'autorisation à ImportHypervisorConfiguration	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
ListGateways	Accorde l'autorisation à ListGateways	Lecture			
ListHypervisors	Accorde l'autorisation à ListHypervisors	Lecture			
ListTagsForResource	Accorde l'autorisation à ListTagsForResource	Lecture	gateway		
			hypervisor		
			virtualmachine		
ListVirtualMachines	Accorde l'autorisation à ListVirtualMachines	Lecture			
PutBandwidthRateLimitSchedule	Accorde l'autorisation à PutBandwidthRateLimitSchedule	Écrire	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutHypervisorPropertyMappings	Accorde l'autorisation à PutHypervisorPropertyMappings	Écrire	hypervisor*		iam:PassRole
PutMaintenanceStartTime	Accorde l'autorisation à PutMaintenanceStartTime	Écrire	gateway*		
Restore	Accorde l'autorisation à Restore	Écrire	hypervisor*		
StartVirtualMachinesMetadataSync	Accorde l'autorisation à StartVirtualMachinesMetadataSync	Écrire	hypervisor*		iam:PassRole
TagResource	Accorde l'autorisation à TagResource	Identification	gateway		
			hypervisor		
			virtualmachine		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestHypervisorConfiguration	Accorde l'autorisation à TestHypervisorConfiguration	Écrire	gateway*		
UntagResource	Accorde l'autorisation à UntagResource	Identification	gateway		
			hypervisor		
			virtualmachine		
				aws:TagKeys	
UpdateGatewayInformation	Accorde l'autorisation à UpdateGatewayInformation	Écrire	gateway*		
UpdateGatewaySoftwareNow	Accorde l'autorisation à UpdateGatewaySoftwareNow	Écrire	gateway*		
UpdateHypervisor	Accorde l'autorisation à UpdateHypervisor	Écrire	gateway*		

Types de ressources définis par AWS Backup Gateway

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
gateway	`arn:${Partition}:backup-gateway:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}
hypervisor	`arn:${Partition}:backup-gateway:${Region}:${Account}:hypervisor/${HypervisorId}`	aws:ResourceTag/${TagKey}
virtualmachine	`arn:${Partition}:backup-gateway:${Region}:${Account}:vm/${VirtualmachineId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Backup Gateway

AWS Backup Gateway définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Backup Search

AWS Backup Search (préfixe de service :`backup-search`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Backup Search
- Types de ressources définis par AWS Backup Search
- Clés de condition pour AWS Backup Search

Actions définies par AWS Backup Search

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSearchJob	Accorde l'autorisation d'obtenir les détails d'une offre d'emploi	Lecture	searchJob*		
GetSearchResultExportJob	Accorde l'autorisation d'obtenir les détails d'une tâche d'exportation des résultats de recherche	Lecture	searchExportJob*		
ListSearchJobBackups	Accorde l'autorisation de répertorier les sauvegardes dans le cadre d'une tâche de recherche	Lecture	searchJob*		
ListSearchJobResults	Accorde l'autorisation de répertorier les résultats d'une tâche de recherche	Lecture	searchJob*		
ListSearchJobs	Accorde l'autorisation de répertorier les offres d'emploi	List			
ListSearchResultExportJobs	Permet de répertorier les tâches d'exportation des résultats de recherche	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	searchExportJob		
			searchJob		
StartSearchJob	Accorde l'autorisation de créer une tâche de recherche	Écrire		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
StartSearchResultExportJob	Autorise le lancement d'une tâche d'exportation pour une tâche de recherche existante	Écrire	searchJob*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopSearchJob	Autorise l'arrêt d'une tâche de recherche en cours	Écrire	searchJob*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	searchExportJob		
			searchJob		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	searchExportJob		
			searchJob		
				aws:TagKeys	

Types de ressources définis par AWS Backup Search

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
searchJob	`arn:${Partition}:backup-search:${Region}:${Account}:search-job/${ResourceId}`	aws:ResourceTag/${TagKey}
searchExportJob	`arn:${Partition}:backup-search:${Region}:${Account}:search-export-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Backup Search

AWS Backup Search définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le stockage des AWS sauvegardes

AWS Le stockage de sauvegarde (préfixe de service :`backup-storage`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Backup storage

- Types de ressources définis par le stockage AWS Backup
- Clés de condition pour le stockage des AWS sauvegardes

Actions définies par AWS Backup storage

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CommitBackupJob [autorisation uniquement]	Accorde l'autorisation de valider une tâche de sauvegarde	Écrire			
DeleteObjects [autorisation uniquement]	Accorde l'autorisation de supprimer des objets	Écrire			
DescribeBackupJob [autorisation uniquement]	Accorde l'autorisation de décrire une tâche de sauvegarde	Écrire			
GetBaseBackup [autorisation uniquement]	Accorde l'autorisation d'obtenir une sauvegarde de base	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetChunk [autorisation uniquement]	Accorde l'autorisation d'obtenir des données à partir d'un point de récupération pour une tâche de restauration	Écrire			
GetIncrementalBaseBackup [autorisation uniquement]	Accorde l'autorisation d'obtenir une sauvegarde de base progressive	Écrire			
GetObjectMetadata [autorisation uniquement]	Accorde l'autorisation d'obtenir des métadonnées à partir d'un point de récupération pour une tâche de restauration	Écrire			
ListChunks [autorisation uniquement]	Accorde l'autorisation de répertorier des données à partir d'un point de récupération pour une tâche de restauration	Écrire			
ListObjects [autorisation uniquement]	Accorde l'autorisation de répertorier des données à partir d'un point de récupération pour une tâche de restauration	Écrire			
MountCapsule [autorisation uniquement]	Associe une clé KMS à un coffre de sauvegarde	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
NotifyObjectComplete [autorisation uniquement]	Accorde l'autorisation de marquer des données téléchargées comme terminées pour une tâche de sauvegarde	Écrire			
PutChunk [autorisation uniquement]	Autorise le téléchargement de données vers un point de restauration AWS géré par sauvegarde pour une tâche de sauvegarde	Écrire			
PutObject [autorisation uniquement]	Accorde l'autorisation de placer un objet	Écrire			
StartObject [autorisation uniquement]	Autorise le téléchargement de données vers un point de restauration AWS géré par sauvegarde pour une tâche de sauvegarde	Écrire			
UpdateObjectComplete [autorisation uniquement]	Accorde l'autorisation de mettre à jour la validation d'un objet	Écrire			

Types de ressources définis par le stockage AWS Backup

AWS Le stockage de sauvegarde ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au stockage AWS Backup, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le stockage des AWS sauvegardes

Le stockage Backup ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Batch

AWS Batch (préfixe de service :`batch`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Batch
- Types de ressources définis par AWS Batch
- Clés de condition pour AWS Batch

Actions définies par AWS Batch

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelJob	Autorise l'annulation d'une tâche dans une file d'attente de tâches AWS Batch de votre compte	Écrire	job*		
CreateComputeEnvironment	Autorise la création d'un environnement de calcul AWS Batch dans votre compte	Écrire	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConsumableResource	Autorise la création d'une ressource consommable AWS Batch dans votre compte	Écrire	consumable-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobQueue	Autorise la création d'une file d'attente de jobs AWS Batch dans votre compte	Écrire	job-queue*		
			compute-e		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			nvironment		
			scheduling-policy		
			service-environment		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuotaShare	Autorise la création d'un partage de quota AWS Batch sur votre compte	Écrire	job-queue*		
			quota-share*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchedulingPolicy	Autorise la création d'une politique de planification AWS par lots dans votre compte	Écrire	scheduling-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceEnvironment	Autorise la création d'un environnement de service AWS Batch dans votre compte	Écrire	service-environment*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComputeEnvironment	Autorise la suppression d'un environnement de calcul AWS Batch dans votre compte	Écrire	compute-environment*		
DeleteConsumableResource	Autorise la suppression d'une ressource consommable AWS Batch dans votre compte	Écrire	consumable-resource*		
DeleteJobQueue	Autorise la suppression d'une file d'attente de jobs AWS Batch dans votre compte	Écrire	job-queue*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteQuotaShare	Autorise la suppression d'une part de quota AWS Batch sur votre compte	Écrire	quota-share*		
DeleteSchedulingPolicy	Autorise la suppression d'une politique de planification AWS par lots dans votre compte	Écrire	scheduling-policy*		
DeleteServiceEnvironment	Autorise la suppression d'un environnement de service AWS Batch dans votre compte	Écrire	service-environment*		
DeregisterJobDefinition	Autorise le désenregistrement d'une définition de tâche AWS Batch dans votre compte	Écrire	job-definition-revision*		
DescribeComputeEnvironments	Autorise à décrire un ou plusieurs environnements de calcul AWS Batch dans votre compte	Lecture			
DescribeConsumableResource	Autorise à décrire une ou plusieurs ressources consommables AWS Batch dans votre compte	Lecture	consumable-resource*		
DescribeJobDefinitions	Accorde l'autorisation de décrire une ou plusieurs définitions de tâches AWS Batch dans votre compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeJobQueues	Permet de décrire une ou plusieurs files d'attente de tâches AWS Batch dans votre compte	Lecture			
DescribeJobs	Accorde l'autorisation de décrire une liste de jobs AWS Batch dans votre compte	Lecture			
DescribeQuotaShare	Autorise à décrire une part de quota AWS Batch sur votre compte	Lecture	quota-share*		
DescribeSchedulingPolicies	Permet de décrire une ou plusieurs politiques de planification AWS par lots dans votre compte	Lecture			
DescribeServiceEnvironments	Autorise à décrire un ou plusieurs environnements de service AWS Batch dans votre compte	Lecture			
DescribeServiceJob	Autorise à décrire une tâche du service AWS Batch dans votre compte	Lecture			
GetJobQueueSnapshot	Accorde l'autorisation d'obtenir un instantané d'une file d'attente de tâches AWS Batch dans votre compte	Lecture	job-queue*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConsumableResources	Permet de répertorier les ressources consommables AWS Batch sur votre compte	List			
ListJobs	Permet de répertorier les tâches pour une file d'attente de tâches AWS Batch spécifiée dans votre compte	List			
ListJobsByConsumableResource	Permet de répertorier les tâches AWS Batch qui nécessitent une ressource consommable spécifique sur votre compte	List	consumable-resource*		
ListQuotaShares	Permet de répertorier les parts de quota AWS Batch sur votre compte	List	job-queue*		
ListSchedulingPolicies	Autorise à répertorier les politiques de planification AWS par lots dans votre compte	Lecture			
ListServiceJobs	Permet de répertorier les tâches de service pour une file d'attente de tâches AWS Batch spécifiée dans votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les tags d'une ressource AWS Batch dans votre compte	Lecture	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			quota-share		
			scheduling-policy		
			service-environment		
			service-job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterJobDefinition	Autorise l'enregistrement d'une définition de tâche AWS Batch dans votre compte	Écrire	job-definition*	aws:ResourceTag/${TagKey}	
			consumable-resource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				batch:User batch:Privileged batch:Image batch:LogDriver batch:AWSLogsGroup batch:AWSLogsRegion batch:AWSLogsStreamPrefix batch:AWSLogsCreateGroup batch:EKSServiceAccountName batch:EKSImage	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				batch:EKSRunAsUser batch:EKSRunAsGroup batch:EKSPrivileged batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	
SubmitJob	Accorde l'autorisation de soumettre une tâche AWS Batch à partir d'une définition de tâche dans votre compte	Écrire	job*	batch:ShareIdentifier batch:EKSImage batch:EKSNamespace	
			job-queue*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			consumable-resource		
			job-definition		
			job-definition-revision		
				aws:RequestTag/${TagKey} aws:TagKeys	
SubmitServiceJob	Accorde l'autorisation de soumettre une tâche de service AWS Batch	Écrire	job-queue*		
			service-job*	batch:ShareIdentifier	
			quota-share		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys batch:SchedulingPriority	
TagResource	Autorise à étiqueter une ressource AWS Batch dans votre compte	Identification	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			quota-share		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			scheduling-policy		
			service-environment		
			service-job		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateJob	Accorde l'autorisation de mettre fin à une tâche dans une file d'attente de tâches AWS Batch de votre compte	Écrire	job*		
TerminateServiceJob	Permet de mettre fin à une tâche de service dans une file d'attente de tâches AWS Batch de votre compte	Écrire	service-job*		
UntagResource	Accorde l'autorisation de supprimer le tag d'une ressource AWS Batch dans votre compte	Identification	compute-environment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			quota-share		
			scheduling-policy		
			service-environment		
			service-job		
				aws:TagKeys	
UpdateComputeEnvironment	Autorise la mise à jour d'un environnement de calcul AWS Batch dans votre compte	Écrire	compute-environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConsumableResource	Autorise la mise à jour d'une ressource consommable AWS Batch dans votre compte	Écrire	consumable-resource*		
UpdateJobQueue	Autorise la mise à jour d'une file d'attente de jobs AWS Batch dans votre compte	Écrire	job-queue*		
			compute-environment		
			scheduling-policy		
UpdateQuotaShare	Autorise la mise à jour d'une part de quota AWS Batch sur votre compte	Écrire	quota-share*		
UpdateSchedulingPolicy	Autorise la mise à jour d'une politique de planification AWS par lots dans votre compte	Écrire	scheduling-policy*		
UpdateServiceEnvironment	Autorise la mise à jour d'un environnement de service AWS Batch dans votre compte	Écrire	service-environment*		
UpdateServiceJob	Autorise la mise à jour d'une tâche de service dans une file d'attente de tâches AWS Batch de votre compte	Écrire	service-job*		
				batch:SchedulingPriority	

Types de ressources définis par AWS Batch

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
compute-environment	`arn:${Partition}:batch:${Region}:${Account}:compute-environment/${ComputeEnvironmentName}`	aws:ResourceTag/${TagKey}
job-queue	`arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}`	aws:ResourceTag/${TagKey}
job-definition	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}`	
job-definition-revision	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:batch:${Region}:${Account}:job/${JobId}`	aws:ResourceTag/${TagKey}
scheduling-policy	`arn:${Partition}:batch:${Region}:${Account}:scheduling-policy/${SchedulingPolicyName}`	aws:ResourceTag/${TagKey}
service-environment	`arn:${Partition}:batch:${Region}:${Account}:service-environment/${ServiceEnvironmentName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
service-job	`arn:${Partition}:batch:${Region}:${Account}:service-job/${JobId}`	aws:ResourceTag/${TagKey}
consumable-resource	`arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}`	aws:ResourceTag/${TagKey}
quota-share	`arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}/quota-share/${QuotaShareName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Batch

AWS Batch définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Clés de condition	Description	Type
batch:AWSLogsCreateGroup	Filtre l'accès en fonction du pilote de journalisation spécifié pour déterminer si le groupe awslogs sera créé pour les journaux	Booléen
batch:AWSLogsGroup	Filtre l'accès en fonction du groupe awslogs où se trouvent les journaux	String
batch:AWSLogsRegion	Filtre l'accès en fonction de la région dans laquelle les journaux sont envoyés	String
batch:AWSLogsStreamPrefix	Filtre l'accès en fonction du préfixe de flux de journaux awslogs	String
batch:EKSImage	Filtre l'accès de l'image utilisée pour démarrer un conteneur pour une tâche Amazon EKS	String
batch:EKSNamespace	Filtre l'accès en fonction de l'espace de noms d'un cluster utilisé pour exécuter le module pour une tâche Amazon EKS	String
batch:EKSPrivileged	Filtre l'accès de la valeur de paramètre privilégié spécifiée qui détermine si le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root) pour une tâche Amazon EKS	Booléen
batch:EKSRunAsGroup	Filtre l'accès de l'identifiant numérique de groupe (gid) spécifié utilisé pour démarrer un conteneur dans une tâche Amazon EKS	Numérique
batch:EKSRunAsUser	Filtre l'accès de l'identifiant numérique utilisateur (uid) spécifié utilisé pour démarrer un conteneur dans une tâche Amazon EKS	Numérique
batch:EKSServiceAccountName	Filtre l'accès du nom du compte de service utilisé pour exécuter le pod pour une tâche Amazon EKS	String

Clés de condition	Description	Type
batch:Image	Filtre l'accès de l'image utilisée pour démarrer un conteneur	String
batch:LogDriver	Filtre l'accès en fonction du pilote de journal utilisé pour le conteneur	String
batch:Privileged	Filtre l'accès en fonction de la valeur de paramètre privilégié spécifiée qui détermine si le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur racine)	Booléen
batch:SchedulingPriority	Filtre l'accès en fonction de la priorité de planification pour les tâches de la file d'attente	Numérique
batch:ShareIdentifier	Filtre l'accès en fonction du shareIdentifier utilisé dans la tâche soumise	String
batch:User	Filtre l'accès en fonction du nom d'utilisateur ou de l'uid numérique utilisé à l'intérieur du conteneur	String

Actions, ressources et clés de condition pour Amazon Bedrock

Amazon Bedrock (préfixe de service : `bedrock`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Bedrock
- Types de ressources définis par Amazon Bedrock

- Clés de condition pour Amazon Bedrock

Actions définies par Amazon Bedrock

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison de journaux vendus pour une base de connaissances	Gestion des autorisations	knowledge-base		
ApplyGuardrail	Donne l'autorisation d'installer un garde-corps	Lecture	guardrail*		
			guardrail-profile		
AssociateAgentCollaborator	Accorde l'autorisation d'associer un autre agent existant en tant que collaborateur à un agent existant	Écrire	agent*		
AssociateAgentKnowledgeBase	Accorde l'autorisation d'associer une base de connaissances à un agent	Écrire	agent*		
			knowledge-base*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateThirdPartyKnowledgeBase [autorisation uniquement]	Accorde l'autorisation d'utiliser une plate-forme tierce pour stocker des données de connaissances	Écrire		bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	
BatchDeleteEvaluationJob	Autorise la suppression par lots de la liste des tâches d'évaluation du socle rocheux	Écrire	evaluation-job*		
CallWithBearerToken	Autorise l'utilisation du jeton porteur	Lecture		bedrock:BearerTokenType	
CancelAutomatedReasoningPolicyBuildWorkflow	Accorde l'autorisation d'annuler un flux de travail de génération pour une politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
CopyBlueprintStage	Permet de copier un plan d'une étape à l'autre	Écrire	blueprint*		
CountTokens	Permet de compter le nombre de jetons dans une invite de saisie	Lecture	foundation-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAgent	Octroie l'autorisation de créer un nouvel agent et un alias d'agent test indiquant la version de l'agent DRAFT.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentActionGroup	Octroie l'autorisation de créer un nouveau groupe d'actions dans un agent existant.	Écrire	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentAlias	Octroie l'autorisation de créer un nouvel alias pour un agent.	Écrire	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomatedReasoningPolicy	Autorise la création d'une nouvelle politique de raisonnement automatique	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAutomatedReasoningPolicyTestCase	Autorise la création d'un scénario de test pour une politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
CreateAutomatedReasoningPolicyVersion	Autorise la création d'une nouvelle version de la politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprint	Accorde l'autorisation de créer un plan pour une sortie personnalisée à partir de l'automatisation des données	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprintVersion	Autorise la création d'une nouvelle version pour un plan existant	Écrire	blueprint*		
CreateCustomModel	Accorde l'autorisation de créer un modèle personnalisé dans Bedrock	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCustomModelDeployment	Accorde l'autorisation de créer un déploiement de modèle personnalisé pour un modèle personnalisé	Écrire	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAutomationProject	Autorise la création d'un projet d'automatisation des données	Écrire	blueprint		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Accorde l'autorisation de créer une source de données.	Écrire	knowledge-base*		
CreateEvaluationJob	Octroie l'autorisation de créer une tâche pour des modèles de fondation d'évaluation ou des modèles personnalisés.	Écrire	custom-model*		
			default-prompt-router*		
			foundation-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			prompt-router*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlow	Accorde l'autorisation de créer un flux rapide	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowAlias	Accorde l'autorisation de créer un alias pour un flux rapide	Écrire	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowVersion	Accorde l'autorisation de créer une version immuable d'un flux rapide	Écrire	flow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFoundationModelAgreement	Accorde l'autorisation de créer un nouveau contrat de modèle de fondation	Écrire			
CreateGuardrail	Octroie l'autorisation de créer une barrière de protection.	Écrire	automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGuardrailVersion	Octroie l'autorisation de créer une version de barrière de protection.	Écrire	guardrail*		
CreateInferenceProfile	Accorde l'autorisation de créer des profils d'inférence	Écrire	application-inference-profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvocation	Accorde l'autorisation de créer un nouvel appel dans une session existante	Écrire	session*		
CreateKnowledgeBase	Accorde l'autorisation de créer une base de connaissances	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMarketplaceModelEndpoint	Accorde l'autorisation de créer un point de terminaison de modèle de marché	Écrire			
CreateModelCopyJob	Accorde l'autorisation de créer une tâche pour copier un modèle personnalisé dans une région ou un compte	Écrire	custom-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelCustomizationJob	Octroie l'autorisation de créer une tâche pour personnaliser le modèle avec vos données d'entraînement personnalisées.	Écrire	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelEvaluationJob	Octroie l'autorisation de créer une tâche pour des modèles de fondation d'évaluation ou des modèles personnalisés.	Écrire	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateModelImportJob	Donne l'autorisation de créer un emploi pour importer un modèle dans Bedrock	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelInvocationJob	Octroie l'autorisation de créer une tâche d'invocation de modèle.	Écrire	custom-model*		
			foundation-model*		
			model-invocation-job*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrompt	Accorde l'autorisation de créer une invite	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePromptRouter	Accorde l'autorisation de créer un routeur d'invite personnalisé	Écrire	application-inference-profile*		
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptVersion	Accorde l'autorisation de créer une version d'une invite	Écrire	prompt*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedModelThroughput	Accorde l'autorisation de créer un nouveau modèle Débit provisionné	Écrire	custom-model*		
			foundation-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSession	Accorde l'autorisation de créer une nouvelle session	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Octroie l'autorisation de supprimer un agent que vous avez créé précédemment.	Écrire	agent*		
DeleteAgentActionGroup	Octroie l'autorisation de supprimer un actionGroup que vous avez créé précédemment.	Écrire	agent*		
DeleteAgentAlias	Autorise la suppression d'une annonce AgentAlias que vous avez créée précédemment	Écrire	agent-alias*		
DeleteAgentMemory	Autorise la suppression de la mémoire existante pour un alias	Écrire	agent-alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAgentVersion	Octroie l'autorisation de supprimer une version d'agent que vous avez créée précédemment.	Écrire	agent*		
DeleteAutomatedReasoningPolicy	Autorise la suppression d'une politique de raisonnement automatique ou de sa version	Écrire	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
DeleteAutomatedReasoningPolicyBuildWorkflow	Accorde l'autorisation de supprimer un flux de travail de génération pour une politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
DeleteAutomatedReasoningPolicyTestCase	Autorise la suppression d'un scénario de test pour une politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
DeleteBlueprint	Autorise la suppression d'un plan pour l'automatisation des données	Écrire	blueprint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCustomModel	Octroie l'autorisation de supprimer un modèle personnalisé que vous avez créé précédemment.	Écrire	custom-model*		
DeleteCustomModelDeployment	Accorde l'autorisation de supprimer un déploiement de modèle personnalisé que vous avez créé précédemment	Écrire	custom-model-deployment*		
DeleteDataAutomationProject	Autorise la suppression d'un projet d'automatisation des données	Écrire	data-automation-project*		
DeleteDataSource	Accorde l'autorisation de supprimer une source de données.	Écrire	knowledge-base*		
DeleteEnforcedGuardrailConfiguration	Autorise la suppression de la configuration de garde-corps imposée au niveau du compte	Écrire			
DeleteFlow	Accorde l'autorisation de supprimer un flux de messages	Écrire	flow*		
DeleteFlowAlias	Accorde l'autorisation de supprimer un alias d'un flux de messages	Écrire	flow-alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFlowVersion	Accorde l'autorisation de supprimer une version d'un flux d'appels	Écrire	flow*		
DeleteFoundationModelAgreement	Accorde l'autorisation de supprimer un contrat de modèle de fondation que vous avez créé précédemment	Écrire			
DeleteGuardrail	Octroie l'autorisation de supprimer une barrière de protection ou sa version.	Écrire	guardrail*		
DeleteImportedModel	Accorde l'autorisation de supprimer le modèle importé Bedrock créé précédemment	Écrire	imported-model*		
DeleteInferenceProfile	Accorde l'autorisation de supprimer des profils d'inférence	Écrire	application-inference-profile*		
DeleteKnowledgeBase	Accorde l'autorisation de supprimer une base de connaissances	Écrire	knowledge-base*		
DeleteKnowledgeBaseDocuments	Accorde l'autorisation de supprimer des documents d'une base de connaissances	Écrire	knowledge-base*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteMarketplaceModelAgreement	Accorde l'autorisation de se désabonner d'un modèle de marché compatible avec Bedrock AWS Marketplace	Écrire			
DeleteMarketplaceModelEndpoint	Autorise la suppression d'un point de terminaison du modèle Marketplace	Écrire	bedrock-marketplace-model-endpoint*		
DeleteModelInvocationLoggingConfiguration	Accorde l'autorisation de supprimer une configuration de journalisation d'invocation	Écrire			
DeletePrompt	Autorise la suppression d'une invite ou de sa version	Écrire	prompt*		
			prompt-version*		
DeletePromptRouter	Accorde l'autorisation de supprimer un routeur d'invite personnalisé	Écrire	prompt-router*		
DeleteProvisionedModelThroughput	Accorde l'autorisation de supprimer un modèle Débit provisionné que vous avez créé précédemment	Écrire	provisioned-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteResourcePolicy [autorisation uniquement]	Supprime une politique de ressources Bedrock créée précédemment	Écrire	custom-model		
			guardrail		
			guardrail-profile		
DeleteSession	Accorde l'autorisation de supprimer une session que vous avez créée précédemment	Écrire	session*		
DeregisterMarketplaceModelEndpoint	Permet de désenregistrer un point de terminaison du modèle de marché pour le rendre inutilisable dans Bedrock Marketplace	Écrire	bedrock-marketplace-model-endpoint*		
DetectGeneratedContent	Accorde l'autorisation de détecter si le contenu fourni est généré à l'aide d'Amazon Bedrock	Lecture	foundation-model*		
DisassociateAgentCollaborator	Accorde l'autorisation de dissocier un collaborateur que vous avez associé précédemment	Écrire	agent*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateAgentKnowledgeBase	Accorde l'autorisation de dissocier une base de connaissances de l'agent	Écrire	agent*		
			knowledge-base*		
EndSession	Accorde l'autorisation de mettre fin à une session que vous avez créée précédemment	Écrire	session*		
ExportAutomatedReasoningPolicyVersion	Accorde l'autorisation de récupérer un artefact de la version d'une politique de raisonnement automatique	Lecture	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
GenerateQuery	Accorde l'autorisation de générer des requêtes associées aux entrées de l'utilisateur	Lecture			
GetAgent	Octroie l'autorisation de récupérer un agent existant.	Lecture	agent*		
GetAgentActionGroup	Octroie l'autorisation de récupérer un groupe d'actions existant.	Lecture	agent*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAgentAlias	Octroie l'autorisation de récupérer un alias existant.	Lecture	agent-alias*		
GetAgentCollaborator	Accorde l'autorisation de récupérer un collaborateur existant	Lecture	agent*		
GetAgentKnowledgeBase	Accorde l'autorisation de décrire une base de connaissances associée à un agent	Lecture	agent*		
			knowledge-base*		
GetAgentMemory	Accorde l'autorisation de récupérer la mémoire existante pour un alias	Lecture	agent-alias*		
GetAgentVersion	Octroie l'autorisation de récupérer une version d'agent existante.	Lecture	agent*		
GetAsyncInvoke	Accorde l'autorisation d'obtenir les propriétés associées à un appel asynchrone que vous avez soumis	Lecture	async-invoke*		
GetAutomatedReasoningPolicy	Accorde l'autorisation de récupérer une politique de raisonnement automatique ou sa version	Lecture	automated-reasoning-policy*		
			automated-reasoning-policy-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAutomatedReasoningPolicyAnnotations	Accorde l'autorisation de récupérer des annotations pour un flux de travail de génération pour une politique de raisonnement automatisée	Lecture	automated-reasoning-policy*		
GetAutomatedReasoningPolicyBuildWorkflow	Accorde l'autorisation de récupérer un flux de travail de génération pour une politique de raisonnement automatisée	Lecture	automated-reasoning-policy*		
GetAutomatedReasoningPolicyBuildWorkflowResultAssets	Accorde l'autorisation de récupérer des ressources pour un flux de travail de création pour une politique de raisonnement automatisée	Lecture	automated-reasoning-policy*		
GetAutomatedReasoningPolicyNextScenario	Accorde l'autorisation de récupérer le prochain scénario généré non révisé pour un flux de travail de génération pour une politique de raisonnement automatique	Lecture	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestCase	Accorde l'autorisation de récupérer un scénario de test pour une politique de raisonnement automatique	Lecture	automated-reasoning-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAutomatedReasoningPolicyTestResult	Accorde l'autorisation de récupérer le résultat d'un scénario de test pour une politique de raisonnement automatique	Lecture	automated-reasoning-policy*		
GetBlueprint	Autorise la récupération d'un plan existant pour l'automatisation des données	Lecture	blueprint*		
GetBlueprintOptimizationStatus	Accorde l'autorisation d'obtenir le statut d'une tâche d'optimisation du plan	Lecture	blueprint-optimization-invocation*		
GetBlueprintRecommendation [autorisation uniquement]	Accorde l'autorisation de récupérer la recommandation du plan	Lecture			
GetCustomModel	Octroie l'autorisation d'obtenir les propriétés associées à un modèle personnalisé Bedrock que vous avez créé.	Lecture	custom-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCustomModelDeployment	Accorde l'autorisation d'obtenir les propriétés associées au déploiement d'un modèle personnalisé. Utilisez cette opération pour obtenir le statut d'un déploiement de modèle personnalisé	Lecture	custom-model-deployment*		
GetDataAutomationProject	Autorise la récupération d'un projet d'automatisation des données existant	Lecture	data-automation-project*		
GetDataAutomationStatus	Accorde l'autorisation de récupérer le statut d'une tâche d'invocation d'automatisation des données	Lecture	data-automation-invocation-job*		
GetDataSource	Accorde l'autorisation de récupérer une source de données existante	Lecture	knowledge-base*		
GetEvaluationJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche d'évaluation. Utilisez cette opération pour obtenir le statut d'une tâche d'évaluation	Lecture	evaluation-job*		
GetExecutionFlowSnapshot	Accorde l'autorisation de récupérer la définition du flux pour une exécution de flux	Lecture	flow*		
			flow-alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			flow-execution*		
GetFlow	Accorde l'autorisation de récupérer un flux d'appels existant	Lecture	flow*		
GetFlowAlias	Accorde l'autorisation de récupérer un alias existant d'un flux d'appels	Lecture	flow-alias*		
GetFlowExecution	Accorde l'autorisation de récupérer une exécution existante d'un alias de flux	Lecture	flow*		
			flow-alias*		
			flow-execution*		
GetFlowVersion	Accorde l'autorisation de récupérer une version existante d'un flux d'appels	Lecture	flow*		
GetFoundationModel	Accorde l'autorisation d'obtenir les propriétés associées à un modèle de fondation Bedrock	Lecture	foundation-model*		
GetFoundationModelAvailability	Accorde l'autorisation d'obtenir la disponibilité d'un modèle de fondation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGuardrail	Octroie l'autorisation de récupérer une barrière de protection ou sa version.	Lecture	guardrail*		
GetImportedModel	Permet d'obtenir les propriétés associées au modèle importé de Bedrock	Lecture	imported-model*		
GetInferenceProfile	Accorde l'autorisation d'obtenir les propriétés associées à un profil d'inférence	Lecture	application-inference-profile*		
			inference-profile*		
GetIngestionJob	Accorde l'autorisation de récupérer une tâche d'ingestion existante	Lecture	knowledge-base*		
GetInvocationStep	Accorde l'autorisation d'obtenir une étape d'invocation depuis une session	Lecture	session*		
GetKnowledgeBase	Accorde l'autorisation de récupérer une base de connaissances existante	Lecture	knowledge-base*		
GetKnowledgeBaseDocuments	Autorise l'accès aux détails des documents d'une base de connaissances	Lecture	knowledge-base*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMarketplaceModelEndpoint	Accorde l'autorisation d'obtenir les propriétés d'un point de terminaison d'un modèle de marché	Lecture	bedrock-marketplace-model-endpoint*		
GetModelCopyJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de copie de modèle. Utilisez cette opération pour obtenir le statut d'une tâche de copie de modèle	Lecture	model-copy-job*		
GetModelCustomizationJob	Octroie l'autorisation d'obtenir les propriétés associées à une tâche de personnalisation de modèle. Utilisez cette opération pour obtenir l'état d'une tâche de personnalisation de modèle.	Lecture	model-customization-job*		
GetModelEvaluationJob	Octroie l'autorisation d'obtenir les propriétés associées à une tâche d'évaluation de modèle. Utilisez cette opération pour obtenir le statut d'une tâche d'évaluation de modèle.	Lecture	model-evaluation-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetModelImportJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche d'importation de modèle et est utilisée pour obtenir le statut d'une tâche d'importation de modèle	Lecture	model-import-job*		
GetModelInvocationJob	Octroie l'autorisation de récupérer une tâche d'invocation de modèle.	Lecture	model-invocation-job*		
GetModelInvocationLoggingConfiguration	Accorde l'autorisation de récupérer une configuration de journalisation d'invocation	Lecture			
GetPrompt	Accorde l'autorisation de récupérer une invite existante ou sa version	Lecture	prompt*		
			prompt-version*		
GetPromptRouter	Accorde l'autorisation d'obtenir les propriétés associées à un routeur rapide	Lecture	default-prompt-router*		
			prompt-router*		
GetProvisionedModelThroughput	Accorde l'autorisation de récupérer modèle Débit provisionné	Lecture	provisioned-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourcePolicy [autorisation uniquement]	Obtient le document de politique de ressources pour une ressource Bedrock	Lecture	custom-model		
			guardrail		
			guardrail-profile		
GetSession	Accorde l'autorisation de récupérer une session existante	Lecture	session*		
GetUseCaseForModelAccess	Accorde l'autorisation de récupérer un cas d'utilisation pour l'accès à un modèle	Lecture			
IngestKnowledgeBaseDocuments	Autorise l'intégration directe de documents dans une base de connaissances	Écrire	knowledge-base*		
InvokeAgent	Octroie l'autorisation d'envoyer des entrées utilisateur (texte uniquement) à l'alias d'un agent pour Bedrock.	Lecture	agent-alias*		
InvokeAutomatedReasoningPolicy [autorisation uniquement]	Accorde l'autorisation d'invoquer une politique de raisonnement automatisé	Lecture	automated-reasoning-policy*		
			automated-reasoning-policy-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvokeBlueprintOptimizationAsync	Accorde l'autorisation d'invoquer une tâche asynchrone pour effectuer l'optimisation du plan	Écrire	blueprint*		
			data-automation-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeBlueprintRecommendationAsync [autorisation uniquement]	Accorde l'autorisation d'invoquer les recommandations du plan de manière asynchrone	Écrire	data-automation-profile*		
InvokeBuilder [autorisation uniquement]	Autorise l'utilisation du générateur conversationnel qui aide à créer des ressources rocheuses soutenues	Écrire			
InvokeDataAutomation	Autorise l'appel à l'API Sync de Bedrock Data Automation	Écrire	blueprint*		
			data-automation-profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			data-automation-project*		
InvokeDataAutomationAsync	Accorde l'autorisation d'invoquer une tâche d'automatisation des données Bedrock	Écrire	blueprint*		
			data-automation-profile*		
			data-automation-project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeFlow	Accorde l'autorisation d'invoquer un flux rapide avec entrée utilisateur	Lecture	flow-alias*		
InvokeInlineAgent	Accorde l'autorisation d'envoyer des entrées utilisateur (texte uniquement) à l'agent en ligne pour Bedrock	Lecture		bedrock:InlineAgentName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvokeModel	Octroie l'autorisation d'invoquer le modèle Bedrock spécifié pour exécuter une inférence à l'aide de l'entrée fournie dans le corps de la demande.	Lecture	application-inference-profile*		
			async-invoke*		
			bedrock-marketplace-model-endpoint*		
			custom-model-deployment*		
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			prompt-router*		
			provisioned-model*		
				bedrock:InferenceProfileArn bedrock:PromptRouterArn aws:RequestTag/${TagKey} aws:TagKeys bedrock:GuardrailIdentifier bedrock:ServiceTier	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvokeModelWithResponseStream	Octroie l'autorisation d'invoquer le modèle Bedrock spécifié pour exécuter une inférence à l'aide de l'entrée fournie dans le corps de la demande avec une réponse de streaming.	Lecture	application-inference-profile*		
			bedrock-marketplace-model-endpoint*		
			custom-model-deployment*		
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			provisioned-model*		
				bedrock:InferenceProfileArn bedrock:PromptRouterArn bedrock:GuardrailIdentifier bedrock:ServiceTier	
InvokeTool	Accorde l'autorisation d'invoquer l'outil Bedrock spécifié pour exécuter l'inférence	Lecture	system-tool*		
ListAgentActionGroups	Octroie l'autorisation de répertorier les groupes d'actions dans un agent.	List	agent*		
ListAgentAliases	Octroie l'autorisation de répertorier des alias pour un agent.	List	agent*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAgentCollaborators	Accorde l'autorisation de répertorier les collaborateurs d'un agent	List	agent*		
ListAgentKnowledgeBases	Accorde l'autorisation de répertorier les bases de connaissances associées à un agent	List	agent*		
ListAgentVersions	Octroie l'autorisation de répertorier des versions d'un agent existantes.	List	agent*		
ListAgents	Octroie l'autorisation de répertorier les agents existants.	List			
ListAsyncInvokes	Accorde l'autorisation d'obtenir une liste des appels asynchrones que vous avez soumis	List			
ListAutomatedReasoningPolicies	Accorde l'autorisation de répertorier les politiques de raisonnement automatique ou leurs versions	List	automated-reasoning-policy		
ListAutomatedReasoningPolicyBuildWorkflows	Autorise la création de listes de flux de travail pour une politique de raisonnement automatisée	List	automated-reasoning-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAutomatedReasoningPolicyTestCases	Accorde l'autorisation de répertorier les cas de test pour une politique de raisonnement automatique	List	automated-reasoning-policy*		
ListAutomatedReasoningPolicyTestResults	Accorde l'autorisation de répertorier les résultats des tests pour une politique de raisonnement automatique	List	automated-reasoning-policy*		
ListBlueprints	Permet de répertorier les plans existants pour l'automatisation des données	List	data-automation-project		
ListCustomModelDeployments	Accorde l'autorisation d'obtenir la liste des déploiements de modèles personnalisés que vous avez soumis	List			
ListCustomModels	Octroie l'autorisation d'obtenir une liste des modèles personnalisés Bedrock que vous avez créés.	List			
ListDataAutomationProjects	Permet de répertorier les projets d'automatisation des données existants	List	blueprint		
ListDataSources	Accorde l'autorisation de répertorier les sources de données existantes dans une base de données	List	knowledge-base*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEnforcedGuardrailsConfiguration	Accorde l'autorisation de répertorier les configurations de garde-corps appliquées au niveau du compte	List			
ListEvaluationJobs	Accorde l'autorisation d'obtenir la liste des tâches d'évaluation que vous avez soumises	List			
ListFlowAliases	Permet de répertorier les alias existants d'un flux rapide	List	flow*		
ListFlowExecutionEvents	Accorde l'autorisation de récupérer des événements pour l'exécution d'un flux	List	flow*		
			flow-alias*		
			flow-execution*		
ListFlowExecutions	Permet de répertorier les exécutions d'un flux ou d'un alias de flux	List	flow*		
			flow-alias		
ListFlowVersions	Accorde l'autorisation de répertorier les versions existantes d'un flux d'appels	List	flow*		
ListFlows	Accorde l'autorisation de répertorier les flux de messages instantanés existants	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFoundationModelAgreementOffers	Accorde l'autorisation d'obtenir une liste des offres de contrats de modèle de fondation	List			
ListFoundationModels	Octroie l'autorisation de répertorier les modèles de fondation Bedrock que vous pouvez utiliser.	List			
ListGuardrails	Octroie l'autorisation de répertorier les barrières de protection ou leurs versions.	List	guardrail		
ListImportedModels	Permet d'obtenir la liste des modèles importés par Bedrock	List			
ListInferenceProfiles	Accorde l'autorisation de répertorier les profils d'inférence que vous pouvez utiliser	List			
ListIngestionJobs	Accorde l'autorisation de répertorier les tâches d'ingestion d'une source de données	List	knowledge-base*		
ListInvocationSteps	Accorde l'autorisation d'obtenir la liste des étapes d'invocation d'une session	List	session*		
ListInvocations	Accorde l'autorisation de répertorier les invocations dans une session	List	session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListKnowledgeBaseDocuments	Accorde l'autorisation de répertorier des documents dans une base de connaissances	List	knowledge-base*		
ListKnowledgeBases	Accorde l'autorisation de répertorier les bases de connaissances existantes	List			
ListMarketplaceModelEndpoints	Accorde l'autorisation de répertorier les points de terminaison du modèle Marketplace que vous pouvez utiliser	Lecture			
ListModelCopyJobs	Accorde l'autorisation d'obtenir la liste des tâches de copie de modèles que vous avez soumises	List			
ListModelCustomizationJobs	Octroie l'autorisation d'obtenir la liste des tâches de personnalisation de modèle que vous avez soumises.	List			
ListModelEvaluationJobs	Octroie l'autorisation d'obtenir la liste des tâches d'évaluation de modèle que vous avez soumises.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListModelImportJobs	Accorde l'autorisation d'obtenir la liste des tâches d'importation de modèles	List			
ListModelInvocationJobs	Octroie l'autorisation de répertorier les tâches d'invocation de modèle que vous avez créées précédemment.	List			
ListPromptRouters	Accorde l'autorisation de répertorier les routeurs rapides que vous pouvez utiliser	List			
ListPrompts	Accorde l'autorisation de répertorier les invites existantes	List	prompt		
ListProvisionedModelThroughputs	Accorde l'autorisation de répertorier les modèles Débit provisionnés que vous avez créés précédemment	List			
ListSessions	Accorde l'autorisation de répertorier les sessions existantes	List			
ListTagsForResource	Octroie l'autorisation de répertorier les balises d'une ressource Bedrock.	Lecture	agent*		
			agent-alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			application-inference-profile*		
			async-invoke*		
			automated-reasoning-policy*		
			automated-reasoning-policy-version*		
			blueprint*		
			blueprint-optimization-invocation*		
			custom-model*		
			custom-model-deployment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			data-automation-invocation-job*		
			data-automation-project*		
			evaluation-job*		
			flow*		
			flow-alias*		
			guardrail*		
			imported-model*		
			knowledge-base*		
			model-copy-job*		
			model-customization-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			model-evaluation-job*		
			model-import-job*		
			model-invocation-job*		
			prompt*		
			prompt-router*		
			prompt-version*		
			provisioned-model*		
			session*		
OptimizePrompt	Accorde l'autorisation d'optimiser une invite avec les entrées de l'utilisateur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PrepareAgent	Octroie l'autorisation de préparer un agent existant à recevoir des demandes d'exécution.	Écrire	agent*		
PrepareFlow	Accorde l'autorisation d'appliquer les dernières modifications apportées à un flux d'invite, afin qu'elles soient prises en compte lors de l'exécution	Écrire	flow*		
PutEnforcedGuardrailConfiguration	Accorde l'autorisation de définir une configuration de garde-corps appliquée au niveau du compte	Écrire			
PutFoundationModelEntitlement	Accorde l'autorisation de donner le droit d'accéder à un modèle de base sans serveur. Ne pas utiliser pour restreindre l'accès aux modèles	Écrire			
PutInvocationStep	Accorde l'autorisation de placer une étape d'invocation dans une invocation en session	Écrire	session*		
PutModelInvocationLoggingConfiguration	Accorde l'autorisation de créer une configuration de journalisation d'invocation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutResourcePolicy [autorisation uniquement]	Ajoute une politique de ressources pour une ressource Bedrock	Écrire	custom-model		
			guardrail		
			guardrail-profile		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutUseCaseForModelAccess	Accorde l'autorisation de saisir un cas d'utilisation pour l'accès à un modèle	Écrire			
RegisterMarketplaceModelEndpoint	Accorde l'autorisation d'enregistrer un point de terminaison Sagemaker en tant que point de terminaison du modèle de marché	Écrire	bedrock-marketplace-model-endpoint*		
RenderPrompt [autorisation uniquement]	Autorise le rendu d'une invite existante ou de sa version	Lecture	prompt*		
			prompt-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Rerank	Accorde l'autorisation de classer les documents en fonction des entrées de l'utilisateur	Écrire			
Retrieve	Octroie l'autorisation de récupérer les données ingérées à partir d'une base de connaissances.	Lecture	knowledge-base*		
RetrieveAndGenerate	Octroie l'autorisation d'envoyer une entrée utilisateur pour effectuer une extraction et une génération.	Écrire			
StartAutomatedReasoningPolicyBuildWorkflow	Accorde l'autorisation de démarrer un flux de travail de génération pour une politique de raisonnement automatisée	Écrire	automated-reasoning-policy*		
StartAutomatedReasoningPolicyTestWorkflow	Accorde l'autorisation de démarrer un flux de travail de test pour une politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
StartFlowExecution	Accorde l'autorisation de démarrer l'exécution d'un alias de flux	Écrire	flow* flow-alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartIngestionJob	Accorde l'autorisation de lancer une tâche d'ingestion	Écrire	knowledge-base*		
StopEvaluationJob	Autorise l'arrêt d'une tâche d'évaluation en cours	Écrire	evaluation-job*		
StopFlowExecution	Accorde l'autorisation d'arrêter l'exécution d'un alias de flux	Écrire	flow*		
			flow-alias*		
			flow-execution*		
StopIngestionJob	Autorise l'arrêt d'une opération d'ingestion	Écrire	knowledge-base*		
StopModelCustomizationJob	Octroie l'autorisation d'arrêter une tâche de personnalisation de modèle Bedrock en cours.	Écrire	model-customization-job*		
StopModelInvocationJob	Octroie l'autorisation d'interrompre une tâche d'invocation de modèle que vous avez lancée précédemment.	Écrire	model-invocation-job*		
TagResource	Octroie l'autorisation de baliser une ressource Bedrock.	Identification	agent		
			agent-alias		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			blueprint-optimization-invocation		
			custom-model		
			custom-model-deployment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			data-automation-invocation-job		
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			model-evaluation-job		
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Octroie l'autorisation de supprimer la balise d'une ressource Bedrock.	Identification	agent		
			agent-alias		
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			blueprint-optimization-invocation		
			custom-model		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			custom-model-deployment		
			data-automation-invocation-job		
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			model-customization-job		
			model-evaluation-job		
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateAgent	Octroie l'autorisation de mettre à jour un agent existant.	Écrire	agent*		
UpdateAgentActionGroup	Octroie l'autorisation de mettre à jour un groupe d'actions existant.	Écrire	agent*		
UpdateAgentAlias	Octroie l'autorisation de mettre à jour un alias existant.	Écrire	agent-alias*		
UpdateAgentCollaborator	Accorde l'autorisation de mettre à jour un collaborateur existant	Écrire	agent*		
UpdateAgentKnowledgeBase	Accorde l'autorisation de mettre à jour une base de connaissances associée à un agent	Écrire	agent* knowledge-base*		
UpdateAutomatedReasoningPolicy	Autorise la mise à jour d'une politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
UpdateAutomatedReasoningPolicyAnnotations	Accorde l'autorisation de mettre à jour les annotations pour un flux de travail de génération pour une politique de raisonnement automatisée	Écrire	automated-reasoning-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAutomatedReasoningPolicyTestCase	Autorise la mise à jour d'un scénario de test pour une politique de raisonnement automatique	Écrire	automated-reasoning-policy*		
UpdateBlueprint	Autorise la mise à jour d'un plan d'automatisation des données	Écrire	blueprint*		
UpdateCustomModelDeployment	Autorise la mise à jour d'un déploiement de modèle personnalisé existant avec un nouveau modèle personnalisé	Écrire	custom-model*		
			custom-model-deployment*		
UpdateDataAutomationProject	Autorise la mise à jour d'un projet d'automatisation des données	Écrire	data-automation-project*		
			blueprint		
UpdateDataSource	Accorde l'autorisation de mettre à jour une source de données	Écrire	knowledge-base*		
UpdateFlow	Accorde l'autorisation de mettre à jour un flux de messages	Écrire	flow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFlowAlias	Accorde l'autorisation de mettre à jour la configuration d'un alias d'un flux rapide	Écrire	flow-alias*		
UpdateGuardrail	Octroie l'autorisation de mettre à jour une barrière de protection.	Écrire	guardrail*		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
UpdateKnowledgeBase	Accorde l'autorisation de mettre à jour une base de connaissances	Écrire	knowledge-base*		
UpdateMarketplaceModelEndpoint	Autorise la mise à jour d'un point de terminaison d'un modèle de marché	Écrire	bedrock-marketplace-model-endpoint*		
UpdatePrompt	Autorise la mise à jour d'une invite	Écrire	prompt*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateProvisionedModelThroughput	Accorde l'autorisation de mettre à jour un modèle Débit provisionné que vous avez créé précédemment	Écrire	custom-model*		
			foundation-model*		
			provisioned-model*		
UpdateSession	Autorise la mise à jour d'une session existante	Écrire	session*		
ValidateFlowDefinition	Accorde l'autorisation de valider les définitions de flux rapides	Lecture			

Types de ressources définis par Amazon Bedrock

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
foundation-model	`arn:${Partition}:bedrock:${Region}::foundation-model/${ResourceId}`	

Types de ressources	ARN	Clés de condition
system-tool	arn:${Partition}:bedrock::${Account}:system-tool/${ResourceId}	
async-invoke	arn:${Partition}:bedrock:${Region}:${Account}:async-invoke/${ResourceId}	aws:ResourceTag/${TagKey}
inference-profile	arn:${Partition}:bedrock:${Region}:${Account}:inference-profile/${ResourceId}	
default-prompt-router	arn:${Partition}:bedrock:${Region}:${Account}:default-prompt-router/${ResourceId}	
prompt-router	arn:${Partition}:bedrock:${Region}:${Account}:prompt-router/${ResourceId}	aws:ResourceTag/${TagKey}
application-inference-profile	arn:${Partition}:bedrock:${Region}:${Account}:application-inference-profile/${ResourceId}	aws:ResourceTag/${TagKey}
custom-model	arn:${Partition}:bedrock:${Region}:${Account}:custom-model/${ResourceId}	aws:ResourceTag/${TagKey}
provisioned-model	arn:${Partition}:bedrock:${Region}:${Account}:provisioned-model/${ResourceId}	aws:ResourceTag/${TagKey}
model-customization-job	arn:${Partition}:bedrock:${Region}:${Account}:model-customization-job/${ResourceId}	aws:ResourceTag/${TagKey}
agent	arn:${Partition}:bedrock:${Region}:${Account}:agent/${AgentId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
agent-alias	arn:${Partition}:bedrock:${Region}:${Account}:agent-alias/${AgentId}/${AgentAliasId}	aws:ResourceTag/${TagKey}
knowledge-base	arn:${Partition}:bedrock:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
model-evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}
evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}
model-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-invocation-job/${JobIdentifier}	aws:ResourceTag/${TagKey}
guardrail	arn:${Partition}:bedrock:${Region}:${Account}:guardrail/${GuardrailId}	aws:ResourceTag/${TagKey}
guardrail-profile	arn:${Partition}:bedrock:${Region}:${Account}:guardrail-profile/${ResourceId}	
automated-reasoning-policy	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}	aws:ResourceTag/${TagKey}
automated-reasoning-policy-version	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}:${AutomatedReasoningPolicyVersion}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
flow	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}	aws:ResourceTag/${TagKey}
flow-alias	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}	aws:ResourceTag/${TagKey}
flow-execution	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}/execution/${FlowExecutionId}	
model-copy-job	arn:${Partition}:bedrock:${Region}:${Account}:model-copy-job/${ResourceId}	aws:ResourceTag/${TagKey}
prompt	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}	aws:ResourceTag/${TagKey}
prompt-version	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}:${PromptVersion}	aws:ResourceTag/${TagKey}
model-import-job	arn:${Partition}:bedrock:${Region}:${Account}:model-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
imported-model	arn:${Partition}:bedrock:${Region}:${Account}:imported-model/${ResourceId}	aws:ResourceTag/${TagKey}
bedrock-marketplace-model-endpoint	arn:${Partition}:bedrock:${Region}:${Account}:marketplace/model-endpoint/all-access	

Types de ressources	ARN	Clés de condition
data-automation-project	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-project/${ProjectId}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:bedrock:${Region}:${Account}:blueprint/${BlueprintId}	aws:ResourceTag/${TagKey}
blueprint-optimization-invocation	arn:${Partition}:bedrock:${Region}:${Account}:blueprint-optimization-invocation/${ResourceId}	aws:ResourceTag/${TagKey}
data-automation-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-invocation/${JobId}	aws:ResourceTag/${TagKey}
data-automation-profile	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-profile/${ProfileId}	
session	arn:${Partition}:bedrock:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
custom-model-deployment	arn:${Partition}:bedrock:${Region}:${Account}:custom-model-deployment/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Bedrock

Amazon Bedrock définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en créant des demandes en fonction de l'ensemble de valeurs autorisé pour chacune des balises obligatoires.	String
aws:ResourceTag/${TagKey}	Filtre l'accès en ayant des actions basées sur la valeur de balise associée à la ressource.	String
aws:TagKeys	Filtre l'accès en créant des demandes en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString
bedrock:BearerTokenType	Filtre l'accès par les jetons porteurs à court ou à long terme	String
bedrock:GuardrailIdentifier	Filtre l'accès en GuardrailIdentifier contenant le Guardrail Arn ou les éléments GuardrailArn suivants : NumericVersion	ARN
bedrock:InferenceProfileArn	Filtre l'accès en fonction du profil d'inférence spécifié	ARN
bedrock:InlineAgentName	Filtre l'accès par les noms d'agents intégrés, cela sera utilisé dans les noms InvokeInlineAgent d'API	String
bedrock:PromptRouterArn	Filtre l'accès par le routeur rapide spécifié	ARN
bedrock:ServiceTier	Filtre l'accès en fonction des paramètres spécifiés ServiceTier	String
bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	Filtre l'accès en fonction du secretArn contenant les informations d'identification de la plate-forme tierce	ARN

Actions, ressources et clés de condition pour Amazon Bedrock Agentcore

Amazon Bedrock Agentcore (préfixe de service :`bedrock-agentcore`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Bedrock Agentcore
- Types de ressources définis par Amazon Bedrock Agentcore
- Clés de condition pour Amazon Bedrock Agentcore

Actions définies par Amazon Bedrock Agentcore

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la télémétrie vendue pour une ressource	Gestion des autorisations	memory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Authorize Action [autorisation uniquement]	Accorde l'autorisation d'évaluer les politiques de Cedar pour les demandes d'autorisation	Gestion des autorisations	gateway*		
			policy-engine*		
BatchCreateMemoryRecords	Accorde l'autorisation de créer un ou plusieurs enregistrements de mémoire	Écrire	memory*		
				bedrock-agentcore:namespace	
BatchDeleteMemoryRecords	Accorde l'autorisation de supprimer un ou plusieurs enregistrements de mémoire	Écrire	memory*		
BatchUpdateMemoryRecords	Autorise la mise à jour d'un ou de plusieurs enregistrements de mémoire	Écrire	memory*		
				bedrock-agentcore:namespace	
CompleteResourceTokenAuth	Accorde l'autorisation de récupérer le jeton d'accès OAuth2 pour que le flux 3LO accède à une ressource externe	Lecture	oauth2credentialprovider*		
			token-vault*		
			workload-identity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workload-identity-directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-agentcore:InboundJwtClaim/iss bedrock-agentcore:InboundJwtClaim/sub bedrock-agentcore:InboundJwtClaim/aud bedrock-agentcore:InboundJwtClaim/scope bedrock-agentcore:InboundJw	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				tClaim/client_id bedrock-agentcore:userid	
ConnectBrowserAutomationStream	Accorde l'autorisation de se connecter à un flux d'automatisation du navigateur	Lecture			
ConnectBrowserLiveViewStream	Accorde l'autorisation de se connecter au flux de visualisation en direct d'un navigateur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAgentRuntime	Accorde l'autorisation de créer un nouvel environnement d'exécution d'agent	Écrire		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:subnets bedrock-agentcore:securityGroups	iam:PassRole
CreateAgentRuntimeEndpoint	Accorde l'autorisation de créer un nouveau point de terminaison d'exécution de l'agent	Écrire	runtime*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApiKeyCredentialProvider	Accorde l'autorisation de créer un nouveau fournisseur d'informations d'identification par clé d'API	Écrire	apikeycredentialprovider*		
			token-vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrowser	Accorde l'autorisation de créer un nouveau navigateur personnalisé	Écrire		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:subnets bedrock-agentcore:securityGroups	
CreateBrowserProfile	Accorde l'autorisation de créer un nouveau profil de navigateur	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCodeInterpreter	Accorde l'autorisation de créer un nouvel interpréteur de code personnalisé	Écrire		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:subnets bedrock-agentcore:securityGroups	
CreateEvaluator	Accorde l'autorisation de créer un nouvel évaluateur	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateEvent	Accorde l'autorisation de créer un événement	Écrire	memory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
CreateGateway	Accorde l'autorisation de créer une nouvelle passerelle	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateGatewayTarget	Autorise la création d'une nouvelle cible dans une passerelle existante	Écrire	gateway*		
CreateMemory	Accorde l'autorisation de créer une ressource de mémoire	Écrire		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:KmsKeyArr	iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOauth2CredentialProvider	Accorde l'autorisation de créer un nouveau fournisseur d'informations d'identification pour accéder aux ressources externes avec OAuth2 le protocole	Écrire	oauth2credentialprovider*		
			token-vault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOnlineEvaluationConfig	Accorde l'autorisation de créer une nouvelle configuration d'évaluation en ligne	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole
CreatePolicy	Accorde l'autorisation de créer une nouvelle politique dans un moteur de politiques	Écrire	policy-engine*		
CreatePolicyEngine	Accorde l'autorisation de créer un nouveau moteur de politiques	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkloadIdentity	Accorde l'autorisation de créer une nouvelle identité de charge de travail	Écrire	workload-identity*		
			workload-identity-directory*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgentRuntime	Autorise la suppression d'un environnement d'exécution d'agent	Écrire	runtime*		
DeleteAgentRuntimeEndpoint	Accorde l'autorisation de supprimer un point de terminaison d'exécution d'un agent	Écrire	runtime*		
			runtime-endpoint*		
DeleteApiKeyCredentialProvider	Accorde l'autorisation de supprimer un fournisseur d'informations d'identification de clé d'API enregistré	Écrire	apikeycredentialprovider*		
			token-vault*		
DeleteBrowser	Accorde l'autorisation de supprimer un navigateur personnalisé	Écrire	browser-custom*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBrowserProfile	Accorde l'autorisation de supprimer un profil de navigateur	Écrire	browser-profile*		
DeleteCodeInterpreter	Accorde l'autorisation de supprimer un interpréteur de code personnalisé	Écrire	code-interpreter-custom*		
DeleteEvaluator	Accorde l'autorisation de supprimer un évaluateur	Écrire	evaluator*		
DeleteEvent	Accorde l'autorisation de supprimer un événement	Écrire	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
DeleteGateway	Autorise la suppression d'une passerelle existante	Écrire	gateway*		
DeleteGatewayTarget	Autorise la suppression d'une cible de passerelle existante	Écrire	gateway*		
DeleteMemory	Accorde l'autorisation de supprimer une ressource de mémoire	Écrire	memory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteMemoryRecord	Autorise la suppression d'un enregistrement mémoire	Écrire	memory*		
DeleteOauth2CredentialProvider	Accorde l'autorisation de supprimer un fournisseur d'OAuth2 informations d'identification enregistré	Écrire	oauth2credentialprovider*		
			token-vault*		
DeleteOnlineEvaluationConfig	Accorde l'autorisation de supprimer une configuration d'évaluation en ligne	Écrire	online-evaluation-config*		
DeletePolicy	Accorde l'autorisation de supprimer une politique	Écrire	policy*		
			policy-engine*		
DeletePolicyEngine	Accorde l'autorisation de supprimer un moteur de politiques	Écrire	policy-engine*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique basée sur les ressources pour une ressource Bedrock	Écrire	gateway		
			runtime		
			runtime-endpoint		
DeleteWorkloadIdentity	Accorde l'autorisation de supprimer une identité de charge de travail enregistrée	Écrire	workload-identity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workload-identity-directory*		
Evaluate	Accorde l'autorisation d'exécuter une évaluation à l'aide d'un évaluateur	Écrire	evaluator*		
GetAgentCard	Autorise à récupérer une carte d'agent pour A2A	Lecture	runtime*		
			runtime-endpoint*		
GetAgentRuntime	Accorde l'autorisation d'obtenir les détails de l'exécution d'un agent	Lecture	runtime*		
GetAgentRuntimeEndpoint	Accorde l'autorisation d'obtenir les détails d'un point de terminaison d'exécution d'un agent	Lecture	runtime*		
			runtime-endpoint*		
GetApiKeyCredentialProvider	Accorde l'autorisation de récupérer un fournisseur d'informations d'identification de clé d'API enregistré par son nom	Lecture	apikeycredentialprovider*		
			token-vault*		
GetBrowser	Accorde l'autorisation d'obtenir les détails d'un navigateur	Lecture	browser-custom*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBrowserProfile	Accorde l'autorisation d'obtenir les détails d'un profil de navigateur	Lecture	browser-profile*		
GetBrowserSession	Accorde l'autorisation d'obtenir les détails d'une session de navigateur	Lecture	browser*		
			browser-custom*		
GetCodeInterpreter	Accorde l'autorisation d'obtenir les détails d'un interpréteur de code	Lecture	code-interpreter-custom*		
GetCodeInterpreterSession	Accorde l'autorisation d'obtenir les détails d'une session d'interpréteur de code	Lecture	code-interpreter*		
			code-interpreter-custom*		
GetEvaluator	Accorde l'autorisation d'obtenir des informations sur un évaluateur	Lecture	evaluator*		
GetEvent	Accorde l'autorisation de récupérer un événement	Lecture	memory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
GetGateway	Accorde l'autorisation de récupérer une passerelle existante	Lecture	gateway*		
GetGatewayTarget	Accorde l'autorisation de récupérer une cible de passerelle existante	Lecture	gateway*		
GetMemory	Accorde l'autorisation de récupérer les détails d'une ressource de mémoire	Lecture	memory*		
GetMemoryRecord	Accorde l'autorisation de récupérer un enregistrement mémoire	Lecture	memory*		
GetOauth2CredentialProvider	Accorde l'autorisation de récupérer un fournisseur d'OAuth2 informations d'identification enregistré par son nom	Lecture	oauth2credentialprovider* token-vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOnlineEvaluationConfig	Accorde l'autorisation d'obtenir les détails d'une configuration d'évaluation en ligne	Lecture	online-evaluation-config*		
GetPolicy	Accorde l'autorisation de récupérer une politique	Lecture	policy*		
			policy-engine*		
GetPolicyEngine	Accorde l'autorisation de récupérer un moteur de politiques	Lecture	policy-engine*		
GetPolicyGeneration	Accorde l'autorisation de récupérer le statut et les résultats d'une demande de génération de politiques	Lecture	policy-engine*		
			policy-generation*		
GetResourceApiKey	Accorde l'autorisation de récupérer une clé d'API associée à un fournisseur d'informations d'identification de clé d'API	Lecture	apikeycredentialprovider*		
			token-vault*		
			workload-identity*		
			workload-identity-directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourceOauth2Token	Accorde l'autorisation de récupérer le jeton d'accès avec un flux OAuth2 2LO ou 3LO pour accéder à une ressource externe	Lecture	oauth2credentialprovider*		
			token-vault*		
			workload-identity*		
			workload-identity-directory*		
GetResourcePolicy	Accorde l'autorisation de récupérer la politique basée sur les ressources pour une ressource Bedrock	Lecture	gateway		
			runtime		
			runtime-endpoint		
GetTokenVault	Accorde l'autorisation de récupérer la configuration actuelle du TokenVault, y compris les paramètres de chiffrement	Lecture	token-vault*		
GetWorkloadAccessToken	Accorde l'autorisation de récupérer un jeton d'accès à une charge de travail pour les charges de travail agentiques n'agissant pas pour le compte d'un utilisateur	Écrire	workload-identity*		
			workload-identity-directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkloadAccessTokenForJWT	Accorde l'autorisation de récupérer un jeton d'accès à la charge de travail pour les charges de travail agentiques agissant au nom de l'utilisateur avec le jeton JWT	Écrire	workload-identity*		
			workload-identity-directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-agentcore:InboundJwtClaim/iss bedrock-agentcore:InboundJwtClaim/sub bedrock-agentcore:InboundJwtClaim/aud bedrock-agentcore:InboundJwtClaim/scope bedrock-agentcore:InboundJw	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				tClaim/client_id	
GetWorkloadAccessTokenForUserId	Accorde l'autorisation de récupérer un jeton d'accès à la charge de travail pour les charges de travail agentic agissant au nom de l'utilisateur ayant un ID utilisateur	Écrire	workload-identity*		
			workload-identity-directory*		
				bedrock-agentcore:userid	
GetWorkloadIdentity	Accorde l'autorisation de récupérer les détails d'une identité de charge de travail spécifique, y compris son nom et le retour autorisé OAuth2 URLs	Lecture	workload-identity*		
			workload-identity-directory*		
InvokeAgentRuntime	Accorde l'autorisation d'invoquer un point de terminaison d'exécution d'un agent	Écrire	runtime*		
			runtime-endpoint*		
InvokeAgentRuntimeCommand	Accorde l'autorisation d'invoquer des commandes sur le point de terminaison d'un agent	Écrire	runtime*		
			runtime-endpoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvokeAgentRuntimeForUser	Accorde l'autorisation d'invoquer un point de terminaison d'exécution d'un agent avec l'Runtime-User-Id en-tête X-Amzn-Bedrock-AgentCore -	Écrire	runtime* runtime-endpoint*		
InvokeAgentRuntimeWithWebSocketStream	Accorde l'autorisation d'invoquer un point de terminaison d'exécution d'un agent avec WebSocket stream	Écrire	runtime* runtime-endpoint*		
InvokeAgentRuntimeWithWebSocketStreamForUser	Accorde l'autorisation d'invoquer un point de terminaison d'exécution d'un agent avec WebSocket stream et avec X-Amzn-Bedrock-AgentCore - Runtime-User-Id header	Écrire	runtime* runtime-endpoint*		
InvokeCodeInterpreter	Accorde l'autorisation d'invoquer une session d'interpréteur de code	Écrire	code-interpreter* code-interpreter-custom*		
InvokeGateway [autorisation uniquement]	Accorde l'autorisation d'invoquer une passerelle	Gestion des autorisations	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListActors	Accorde l'autorisation de répertorier les acteurs	List	memory*		
ListAgentRuntimeEndpoints	Accorde l'autorisation de répertorier les points de terminaison d'exécution de l'agent	List			
ListAgentRuntimeVersions	Accorde l'autorisation de répertorier les versions d'exécution de l'agent	List			
ListAgentRuntimes	Accorde l'autorisation de répertorier les environnements d'exécution des agents	List			
ListApiKeyCredentialProviders	Accorde l'autorisation de répertorier tous les fournisseurs d'identifiants clés d'API dans le Token Vault	Lecture	apikeycredentialprovider*		
			token-vault*		
ListBrowserProfiles	Accorde l'autorisation de répertorier les profils de navigateur	List			
ListBrowserSessions	Accorde l'autorisation de répertorier les sessions du navigateur	List			
ListBrowsers	Accorde l'autorisation de répertorier les navigateurs	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCodeInterpreterSessions	Accorde l'autorisation de répertorier les sessions d'interprétation de code	List	code-interpreter*		
			code-interpreter-custom*		
ListCodeInterpreters	Accorde l'autorisation de répertorier les interprètes de code	List			
ListEvaluators	Accorde l'autorisation de répertorier les évaluateurs	List			
ListEvents	Accorde l'autorisation de répertorier des événements	List	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
ListGatewayTargets	Accorde l'autorisation de répertorier les cibles de passerelle existantes	List	gateway*		
ListGateways	Accorde l'autorisation de répertorier les passerelles existantes	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMemories	Accorde l'autorisation de répertorier les ressources de mémoire	List			
ListMemoryExtractionJobs	Permet de répertorier les tâches d'extraction pour cette mémoire	List	memory*		
ListMemoryRecords	Accorde l'autorisation de répertorier les enregistrements en mémoire	List	memory*		
				bedrock-agentcore:namespace bedrock-agentcore:strategyId	
ListOauth2CredentialProviders	Permet de répertorier tous les fournisseurs OAuth2 d'informations d'identification dans le Token Vault	Lecture	oauth2credentialprovider*		
			token-vault*		
ListOnlineEvaluationConfigs	Accorde l'autorisation de répertorier les configurations d'évaluation en ligne	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPolicies	Accorde l'autorisation de répertorier les politiques dans un moteur de politiques	List	policy-engine*		
ListPolicyEngines	Accorde l'autorisation de répertorier les moteurs de politiques	List			
ListPolicyGenerationAssets	Accorde l'autorisation de répertorier les actifs de politique générés à partir d'une demande de génération	List	policy-engine*		
			policy-generation*		
ListPolicyGenerations	Accorde l'autorisation de répertorier les demandes de génération de politiques	List	policy-engine*		
ListSessions	Accorde l'autorisation de répertorier les sessions	List	memory*		
				bedrock-agentcore:actorId	
ListTagsForResource	Accorde l'autorisation de répertorier les tags d'une ressource Bedrock AgentCore	List	apikeycredentialprovider		
			browser-custom		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			browser-profile		
			code-interpreter-custom		
			evaluator		
			gateway		
			memory		
			oauth2credentialprovider		
			online-evaluation-config		
			runtime		
			runtime-endpoint		
			token-vault		
			workload-identity		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workload-identity-directory		
ListWorkloadIdentities	Accorde l'autorisation de répertorier toutes les identités de charge de travail dans le fichier de l'appelant Compte AWS	Lecture	workload-identity*		
			workload-identity-directory*		
ManageAdminPolicy [autorisation uniquement]	Accorde l'autorisation de créer ou de modifier des politiques génériques qui s'appliquent aux ressources de passerelle	Gestion des autorisations			
ManageResourceScopedPolicy [autorisation uniquement]	Accorde l'autorisation de créer ou de modifier des politiques qui s'appliquent à des ressources de passerelle spécifiques	Gestion des autorisations	gateway*		
PartiallyAuthorizeActions [autorisation uniquement]	Accorde l'autorisation d'effectuer une évaluation partielle des politiques de Cedar afin d'autoriser un appelant à répertorier les outils qu'il est autorisé à appeler	Gestion des autorisations	gateway*		
			policy-engine*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutResourcePolicy	Accorde l'autorisation de créer ou de mettre à jour la politique basée sur les ressources pour une ressource Bedrock	Écrire	gateway		
			runtime		
			runtime-endpoint		
RetrieveMemoryRecords	Accorde l'autorisation de récupérer des enregistrements de mémoire par le biais d'une requête sémantique	List	memory*		
				bedrock-agentcore:namespace bedrock-agentcore:strategyId	
SaveBrowserSessionProfile	Accorde l'autorisation d'enregistrer un profil de session de navigateur	Écrire	browser*		
			browser-custom*		
			browser-profile*		
SetTokenVaultCMK	Accorde l'autorisation d'associer une clé gérée par le client (CMK) ou une clé gérée par un service à un TokenVault	Lecture	token-vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartBrowserSession	Accorde l'autorisation de démarrer une nouvelle session de navigateur	Écrire	browser*		
			browser-custom*		
			browser-profile		
StartCodeInterpreterSession	Accorde l'autorisation de démarrer une nouvelle session d'interpréteur de code	Écrire	code-interpreter*		
			code-interpreter-custom*		
StartMemoryExtractionJob	Autorise le démarrage de la tâche d'extraction de mémoire	Écrire	memory*		
				bedrock-agentcore:strategyId bedrock-agentcore:sessionId bedrock-agentcore:actorId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartPolicyGeneration	Autorise le lancement d'une demande de génération de politiques basée sur l'IA	Écrire	policy-engine*		
StopBrowserSession	Accorde l'autorisation d'arrêter une session de navigateur	Écrire	browser*		
			browser-custom*		
StopCodeInterpreterSession	Autorise l'arrêt d'une session d'interpréteur de code	Écrire	code-interpreter*		
			code-interpreter-custom*		
StopRuntimeSession	Autorise l'arrêt d'une session d'exécution	Écrire	runtime*		
			runtime-endpoint*		
SynchronizeGatewayTargets [autorisation uniquement]	Accorde l'autorisation d'activer la recherche sur les passerelles	Gestion des autorisations	gateway*		
TagResource	Accorde l'autorisation de taguer une ressource Bedrock AgentCore	Identification	apikeycredentialprovider		
			browser-custom		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			browser-profile		
			code-interpreter-custom		
			evaluator		
			gateway		
			memory		
			oauth2credentialprovider		
			online-evaluation-config		
			runtime		
			runtime-endpoint		
			token-vault		
			workload-identity		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workload-identity-directory		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Permet de détaguer une ressource Bedrock AgentCore	Identification	apikeycredentialprovider		
			browser-custom		
			browser-profile		
			code-interpreter-custom		
			evaluator		
			gateway		
			memory		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			oauth2credentialprovider		
			online-evaluation-config		
			runtime		
			runtime-endpoint		
			token-vault		
			workload-identity		
			workload-identity-directory		
				aws:TagKeys	
UpdateAgentRuntime	Autorise la mise à jour de l'environnement d'exécution d'un agent	Écrire	runtime*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-agentcore:subnets bedrock-agentcore:securityGroups	
UpdateAgentRuntimeEndpoint	Accorde l'autorisation de mettre à jour le point de terminaison d'un agent	Écrire	runtime*		
			runtime-endpoint*		
UpdateApiKeyCredentialProvider	Autorise la mise à jour d'un fournisseur d'identifiants de clé d'API existant	Écrire	apikeycredentialprovider*		
			token-vault*		
UpdateBrowserStream	Autorise la mise à jour de l'état du flux de session du navigateur	Écrire	browser*		
			browser-custom*		
UpdateEvaluator	Accorde l'autorisation de mettre à jour un évaluateur	Écrire	evaluator*		
UpdateGateway	Autorise la mise à jour d'une passerelle existante	Écrire	gateway*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGatewayTarget	Autorise la mise à jour d'une cible de passerelle existante	Écrire	gateway*		
UpdateMemory	Autorise la mise à jour d'une ressource de mémoire	Écrire	memory*		iam:PassRole
UpdateOauth2CredentialProvider	Autorise la mise à jour d'un fournisseur d' OAuth2 informations d'identification existant	Écrire	oauth2credentialprovider*		
			token-vault*		
UpdateOnlineEvaluationConfig	Autorise la mise à jour d'une configuration d'évaluation en ligne	Écrire	online-evaluation-config*		iam:PassRole
UpdatePolicy	Autorise la mise à jour d'une politique existante	Écrire	policy*		
			policy-engine*		
UpdatePolicyEngine	Autorise la mise à jour d'un moteur de politiques	Écrire	policy-engine*		
UpdateWorkloadIdentity	Autorise la mise à jour des métadonnées d'une identité de charge de travail existante	Écrire	workload-identity*		
			workload-identity-directory*		

Types de ressources définis par Amazon Bedrock Agentcore

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
evaluator	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:evaluator/${EvaluatorId}`	aws:ResourceTag/${TagKey}
online-evaluation-config	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:online-evaluation-config/${OnlineEvaluationConfigId}`	aws:ResourceTag/${TagKey}
memory	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:memory/${MemoryId}`	aws:ResourceTag/${TagKey}
gateway	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}
workload-identity	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}/workload-identity/${WorkloadIdentityName}`	aws:ResourceTag/${TagKey}
oauth2credentialprovider	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/oauth2credentialprovider/${Name}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
apikeycredentialprovider	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/apikeycredentialprovider/${Name}	aws:ResourceTag/${TagKey}
runtime	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}	aws:ResourceTag/${TagKey}
runtime-endpoint	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}/runtime-endpoint/${Name}	aws:ResourceTag/${TagKey}
code-interpreter-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:code-interpreter-custom/${CodeInterpreterId}	aws:ResourceTag/${TagKey}
code-interpreter	arn:${Partition}:bedrock-agentcore:${Region}:aws:code-interpreter/${CodeInterpreterId}	
browser-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:browser-custom/${BrowserId}	aws:ResourceTag/${TagKey}
browser	arn:${Partition}:bedrock-agentcore:${Region}:aws:browser/${BrowserId}	
browser-profile	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:browser-profile/${BrowserProfileId}	aws:ResourceTag/${TagKey}
workload-identity-directory	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
token-vault	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}	aws:ResourceTag/${TagKey}
policy-engine	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:policy-engine/${PolicyEngineId}	
policy	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:policy-engine/${PolicyEngineId}/policy/${PolicyId}	
policy-generation	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:policy-engine/${PolicyEngineId}/policy-generation/${PolicyGenerationId}	

Clés de condition pour Amazon Bedrock Agentcore

Amazon Bedrock Agentcore définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en créant des demandes en fonction de l'ensemble de valeurs autorisé pour chacune des balises obligatoires.	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en ayant des actions basées sur la valeur de balise associée à la ressource.	String
aws:TagKeys	Filtre l'accès en créant des demandes en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString
bedrock-agentcore:GatewayAuthorizerType	Filtre l'accès par l'attribut AuthorizerType sur une passerelle	String
bedrock-agentcore:InboundJwtClaim/aud	Filtre l'accès en fonction de l'audience (aud) dans le JWT transmis dans la demande	ArrayOfString
bedrock-agentcore:InboundJwtClaim/client_id	Filtre l'accès par la réclamation client_id dans le JWT transmis dans la demande	String
bedrock-agentcore:InboundJwtClaim/iss	Filtre l'accès par l'émetteur (iss) à la réclamation présente dans le JWT transmis dans la demande	String
bedrock-agentcore:InboundJwtClaim/scope	Filtre l'accès en fonction de la demande de portée dans le JWT transmis dans la demande	ArrayOfString
bedrock-agentcore:InboundJwtClaim/sub	Filtre l'accès en fonction de l'objet de la réclamation (sous) dans le JWT transmis dans la demande	String

Clés de condition	Description	Type
bedrock-agentcore:KmsKeyArn	Filtre l'accès par le biais du code KMS fourni	String
bedrock-agentcore:actorId	Filtre l'accès par identifiant d'acteur	String
bedrock-agentcore:namespace	Filtre l'accès par espace de noms	String
bedrock-agentcore:securityGroups	Filtre l'accès en fonction de l'ID des groupes de sécurité configurés pour l' AgentCore environnement d'exécution	ArrayOfString
bedrock-agentcore:sessionId	Filtre l'accès par identifiant de session	String
bedrock-agentcore:strategyId	Filtre l'accès par ID de stratégie de mémoire	String
bedrock-agentcore:subnets	Filtre l'accès en fonction de l'ID des sous-réseaux configurés pour l'exécution AgentCore	ArrayOfString
bedrock-agentcore:userid	Filtre l'accès en fonction de la valeur d'ID utilisateur statique transmise dans la demande	String

Actions, ressources et clés de condition pour Amazon Bedrock Powered by AWS Mantle

Amazon Bedrock Powered by AWS Mantle (préfixe de service :`bedrock-mantle`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Bedrock Powered by AWS Mantle
- Types de ressources définis par Amazon Bedrock Powered by AWS Mantle
- Clés de condition pour Amazon Bedrock Powered by AWS Mantle

Actions définies par Amazon Bedrock Powered by AWS Mantle

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ArchiveProject	Accorde l'autorisation d'archiver un projet spécifique	Écrire	project*	aws:ResourceTag/${TagKey}	
AssociateCustomizedModel	Accorde l'autorisation d'associer un modèle personnalisé à un projet	Écrire	customized-model*	aws:ResourceTag/${TagKey}	
			project*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-mantle:ProjectArn bedrock-mantle:CustomizedModelArn	
CallWithBearerToken [autorisation uniquement]	Accorde l'autorisation d'effectuer des appels d'API à l'aide de l'authentification par jeton porteur	List		bedrock-mantle:BearerTokenType	
CancelFineTuningJob	Autorise l'annulation d'une tâche de réglage fin en cours	Écrire	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:FineTuningJob	
CancelInference	Autorise l'annulation d'une demande d'inférence en cours	Écrire	project*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCustomizedModel	Autorise l'importation d'un modèle personnalisé avec des poids personnalisés	Écrire	customized-model*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFile	Accorde l'autorisation de créer un fichier dans un projet	Écrire	project*	aws:ResourceTag/${TagKey}	
CreateFineTuningJob	Accorde l'autorisation de créer une tâche de réglage précis	Écrire	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:Model bedrock-mantle:Files	
CreateInference	Accorde l'autorisation de créer une demande d'inférence de fin de chat	Écrire	project*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-mantle:ServiceTier bedrock-mantle:Model	
CreateProject	Accorde l'autorisation de créer un projet	Écrire	project*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReservation	Accorde l'autorisation de créer une réservation de capacité pour un modèle	Écrire	project*	aws:ResourceTag/${TagKey}	
			reservation*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys bedrock-mantle:ProjectArn bedrock-mantle:ReservationArn	
DeleteCustomizedModel	Accorde l'autorisation de supprimer un modèle personnalisé	Écrire	customized-model*	aws:ResourceTag/${TagKey}	
DeleteFile	Accorde l'autorisation de supprimer un fichier spécifique	Écrire	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:Files	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteInference	Accorde l'autorisation de supprimer une demande d'inférence spécifique	Écrire	project*	aws:ResourceTag/${TagKey}	
DeleteReservation	Accorde l'autorisation de supprimer une réserve de capacité	Écrire	project*	aws:ResourceTag/${TagKey}	
			reservation*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:ProjectArn	
				bedrock-mantle:ReservationArn	
DisassociateCustomizedModel	Accorde l'autorisation de dissocier un modèle personnalisé d'un projet	Écrire	customized-model*	aws:ResourceTag/${TagKey}	
			project*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-mantle:ProjectArn bedrock-mantle:CustomizedModelArn	
GetCustomizedModel	Accorde l'autorisation d'obtenir un modèle personnalisé	Lecture	customized-model*	aws:ResourceTag/${TagKey}	
GetFile	Accorde l'autorisation de récupérer des informations sur un fichier spécifique	Lecture	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:Files	
GetFineTuningJob	Accorde l'autorisation de récupérer les détails d'une tâche de réglage précise	Lecture	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:FineTuningJob	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInference	Accorde l'autorisation de récupérer les détails d'une demande d'inférence spécifique	Lecture	project*	aws:ResourceTag/${TagKey}	
GetModel	Accorde l'autorisation de récupérer des informations sur un modèle spécifique	Lecture	project*	aws:ResourceTag/${TagKey}	
GetProject	Accorde l'autorisation de récupérer les détails d'un projet spécifique	Lecture	project*	aws:ResourceTag/${TagKey}	
GetReservation	Accorde l'autorisation d'obtenir une réservation	Lecture	reservation*	aws:ResourceTag/${TagKey}	
ListCustomizedModelAssociations	Accorde l'autorisation de répertorier les associations de projets pour un modèle personnalisé	List	customized-model*		
ListCustomizedModels	Autorise la mise en vente de modèles personnalisés	List	customized-model*		
ListFiles	Accorde l'autorisation de répertorier tous les fichiers disponibles dans un projet	List	project*	aws:ResourceTag/${TagKey}	
ListFineTuningJobs	Permet de répertorier toutes les tâches de réglage fin disponibles dans un projet	List	project*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListModels	Permet de répertorier tous les modèles disponibles dans un projet	List	project*	aws:ResourceTag/${TagKey}	
ListProjects	Accorde l'autorisation de répertorier les projets	List	project*		
ListReservations	Accorde l'autorisation de répertorier les réservations.	List	reservation*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	customized-model	aws:ResourceTag/${TagKey}	
			project	aws:ResourceTag/${TagKey}	
			reservation	aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	customized-model	aws:ResourceTag/${TagKey}	
			project	aws:ResourceTag/${TagKey}	
			reservation	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	customized-model	aws:ResourceTag/${TagKey}	
			project	aws:ResourceTag/${TagKey}	
			reservation	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateProject	Autorise la mise à jour d'un projet spécifique	Écrire	project*	aws:ResourceTag/${TagKey}	
UpdateReservation	Autorise la mise à jour de la réservation	Écrire	project*	aws:ResourceTag/${TagKey}	
			reservation*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				bedrock-mantle:ProjectArn bedrock-mantle:ReservationArn	

Types de ressources définis par Amazon Bedrock Powered by AWS Mantle

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
project	`arn:${Partition}:bedrock-mantle:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}
customized-model	`arn:${Partition}:bedrock-mantle:${Region}:${Account}:customized-model/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
reservation	`arn:${Partition}:bedrock-mantle:${Region}:${Account}:reservation/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Bedrock Powered by AWS Mantle

Amazon Bedrock Powered by AWS Mantle définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
bedrock-mantle:BearerTokenType	Filtre l'accès par les jetons porteurs à court ou à long terme	String
bedrock-mantle:CustomizedModelArn	Filtre l'accès par l'ARN du modèle personnalisé associé ou référencé dans les opérations entre ressources	String

Clés de condition	Description	Type
bedrock-mantle:Files	Filtre l'accès en fonction des identifiants de fichiers spécifiés	ArrayOfString
bedrock-mantle:FineTuningJob	Filtre l'accès en fonction de l'identifiant de tâche de réglage précis spécifié	String
bedrock-mantle:Model	Filtre l'accès selon le modèle spécifié	String
bedrock-mantle:ProjectArn	Filtre l'accès par l'ARN du projet associé ou référencé dans les opérations inter-ressources	String
bedrock-mantle:ReservationArn	Filtre l'accès par l'ARN de la réservation référencée dans les opérations entre ressources	String
bedrock-mantle:ServiceTier	Filtre l'accès en fonction des paramètres spécifiés ServiceTier	String

Actions, ressources et clés de condition pour AWS Billing

AWS Billing (préfixe de service :`billing`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Billing
- Types de ressources définis par AWS Billing
- Clés de condition pour AWS Billing

Actions définies par AWS Billing

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateSourceViews	Accorde l'autorisation d'associer des vues de source à une vue de facturation	Écrire	billingview*		billing:UseSourceView iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
CreateBillingView	Accorde l'autorisation de créer une vue de facturation	Écrire	billingview*		billing:UseSourceView iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DeleteBillingView	Accorde l'autorisation de supprimer une vue de facturation	Écrire	billingview*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer une politique de ressources d'affichage de facturation	Gestion des autorisations	billingview*		
				aws:ResourceTag/${TagKey}	
DisassociateSourceViews	Accorde l'autorisation de dissocier les vues source d'une vue de facturation	Écrire	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingData [autorisation uniquement]	Accorde l'autorisation d'exécuter des requêtes sur les informations de facturation	Lecture	billingview		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBillingDetails [autorisation uniquement]	Accorde l'autorisation d'afficher les informations de facturation détaillées du élément de ligne	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
GetBillingNotifications [autorisation uniquement]	Accorde l'autorisation de consulter les notifications envoyées par le AWS biais des informations de facturation de votre compte	Lecture			
GetBillingPreferences [autorisation uniquement]	Autorise à consulter les préférences de facturation telles que les instances réservées, les Savings Plans (plans d'épargne) et le partage de crédits	Lecture			
GetBillingView	Accorde l'autorisation d'obtenir les métadonnées pour une vue de facturation spécifiée	Lecture	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingViewData [autorisation uniquement]	Autorise l'accès aux données de coût et d'utilisation pour une vue de facturation spécifiée	Lecture	billingview*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContractInformation [autorisation uniquement]	Autorise à consulter les informations contractuelles du compte, y compris le numéro de contrat, les noms des organisations utilisatrices finales, les numéros de commande et si le compte est utilisé pour servir des clients du secteur public	Lecture			
GetCredits [autorisation uniquement]	Autorise à consulter les crédits qui ont été utilisés	Lecture			
GetIAMAccessPreference [autorisation uniquement]	Accorde l'autorisation de récupérer l'état de la préférence de facturation Allow IAM Access	Lecture			
GetResourcePolicy	Accorde l'autorisation d'obtenir la vue de facturation spécifiée dans la politique de ressources	Gestion des autorisations	billingview*		
				aws:ResourceTag/${TagKey}	
GetSellerOfRecord [autorisation uniquement]	Accorde l'autorisation de récupérer le vendeur enregistré par défaut du compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBillingViews	Accorde l'autorisation d'obtenir une liste de toutes les vues de facturation disponibles	Lecture			
ListSourceViewsForBillingView	Accorde l'autorisation d'obtenir la liste des vues source pour une vue de facturation spécifiée	List	billingview*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Accorde l'autorisation d'obtenir la liste des tags pour une vue de facturation spécifiée	Lecture	billingview*		
				aws:ResourceTag/${TagKey}	
PutContractInformation [autorisation uniquement]	Autorise à définir les informations contractuelles du compte, les noms des organisations utilisatrices finales, et si le compte est utilisé pour servir des clients du secteur public	Écrire			
PutResourcePolicy [autorisation uniquement]	Autorise la mise en place d'une politique de ressources d'affichage de facturation	Gestion des autorisations	billingview*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RedeemCredits [autorisation uniquement]	Donne l'autorisation de racheter n'importe quel crédit AWS	Écrire			
TagResource	Accorde l'autorisation d'ajouter des tags à une vue de facturation spécifiée	Identification	billingview*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer un tag d'une vue de facturation spécifiée	Identification	billingview*		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateBillingPreferences [autorisation uniquement]	Autorise à mettre à jour les préférences de facturation telles que les instances réservées, les Savings Plan (plans d'épargne) et le partage de crédits	Écrire			
UpdateBillingView	Autorise la mise à jour d'une vue de facturation	Écrire	billingview*		
				aws:ResourceTag/${TagKey}	
UpdateIAMAccessPreference [autorisation uniquement]	Accorde l'autorisation de mettre à jour la préférence de facturation Allow IAM Access	Écrire			
UseSourceView [autorisation uniquement]	Autorise l'utilisation d'une vue de facturation comme source de données pour d'autres vues de facturation	Lecture			

Types de ressources définis par AWS Billing

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Billing

AWS Billing définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les tableaux AWS Billing de bord de gestion des coûts

AWS Billing et les tableaux de bord de gestion des coûts (préfixe de service :`bcm-dashboards`) fournissent les ressources, les actions et les clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Billing et tableaux de bord de gestion des coûts
- Types de ressources définis par AWS Billing et tableaux de bord de gestion des coûts
- Clés de condition AWS Billing et tableaux de bord de gestion des coûts

Actions définies par AWS Billing et tableaux de bord de gestion des coûts

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDashboard	Accorde l'autorisation de créer un tableau de bord	Écrire			
DeleteDashboard	Accorde l'autorisation de supprimer un tableau de bord	Écrire			
GetDashboard	Accorde l'autorisation d'obtenir les informations du tableau de bord	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourcePolicy	Accorde l'autorisation d'obtenir la politique de ressources pour un tableau de bord	Lecture			
ListDashboards	Accorde l'autorisation de répertorier les informations relatives à tous les tableaux de bord d'un utilisateur	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier tous les tags d'une ressource	Lecture			
TagResource	Accorde l'autorisation de créer un tag pour une ressource	Identification		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer un tag pour une ressource	Identification		aws:TagKeys	
UpdateDashboard	Autorise la mise à jour d'un tableau de bord existant	Écrire			

Types de ressources définis par AWS Billing et tableaux de bord de gestion des coûts

AWS Billing et Cost Management Dashboards ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès aux tableaux de bord de gestion des coûts AWS Billing et leur accès, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition AWS Billing et tableaux de bord de gestion des coûts

AWS Billing et Cost Management Dashboards définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les exportations AWS Billing de données de gestion des coûts

AWS Billing Et les exportations de données de gestion des coûts (préfixe de service :`bcm-data-exports`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Billing And Cost Management Data Exports
- Types de ressources définis par AWS Billing And Cost Management Data Exports
- Clés de condition pour les exportations de données AWS Billing et de gestion des coûts

Actions définies par AWS Billing And Cost Management Data Exports

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExport	Octroie l'autorisation de créer une exportation.	Écrire	table*		
			billingview		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExport	Octroie l'autorisation de supprimer une exportation.	Écrire	export*		
				aws:ResourceTag/${TagKey}	
GetExecution	Octroie l'autorisation d'obtenir l'exécution d'une exportation.	Lecture	export*		
				aws:ResourceTag/${TagKey}	
GetExport	Octroie l'autorisation d'obtenir une exportation.	Lecture	export*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetTable	Octroie l'autorisation d'obtenir les informations relatives à une table.	Lecture	table*		
ListExecutions	Octroie l'autorisation de répertorier toutes les exécutions d'une exportation.	List	export*		
				aws:ResourceTag/${TagKey}	
ListExports	Octroie l'autorisation de répertorier toutes les exportations.	List			
ListTables	Octroie l'autorisation de répertorier toutes les tables disponibles.	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	export*		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	export*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	export*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateExport	Octroie l'autorisation de mettre à jour une exportation.	Écrire	export*		
			table*		
			billingview		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS Billing And Cost Management Data Exports

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
export	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:export/${Identifier}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:bcm-data-exports:${Region}:${Account}:table/${Identifier}`	
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les exportations de données AWS Billing et de gestion des coûts

AWS Billing Et les exportations de données de gestion des coûts définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le calculateur de prix AWS Billing And Cost Management

AWS Billing Et le calculateur de tarification de la gestion des coûts (préfixe de service :`bcm-pricing-calculator`) fournit les ressources, les actions et les clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Billing And Cost Management Pricing Calculator
- Types de ressources définis par AWS Billing And Cost Management Pricing Calculator
- Clés de condition pour le calculateur de prix AWS Billing And Cost Management

Actions définies par AWS Billing And Cost Management Pricing Calculator

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBillEstimate	Accorde l'autorisation de créer une nouvelle estimation de facture. Des frais sont facturés pour des estimations de factures réussies	Écrire	bill-scenario		
CreateBillScenario	Autorise la création d'un nouveau scénario de facturation	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBillScenarioCommitmentModification	Accorde l'autorisation de créer de nouveaux engagements ou de supprimer un engagement existant dans un scénario de facturation spécifié	Écrire	bill-scenario*		
CreateBillScenarioUsageModification	Accorde l'autorisation de créer un usage dans le scénario de facturation spécifié	Écrire	bill-scenario*		
CreateWorkloadEstimate	Autorise la création d'une nouvelle estimation de la charge de travail	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkloadEstimateUsage	Accorde l'autorisation de créer une utilisation dans l'estimation de charge de travail spécifiée	Écrire	workload-estimate*		
DeleteBillEstimate	Autorise la suppression de l'estimation de facture	Écrire	bill-estimate*		
DeleteBillScenario	Autorise la suppression d'un scénario de facture	Écrire	bill-scenario*		
DeleteBillScenarioCommitmentModification	Accorde l'autorisation de supprimer les engagements récemment ajoutés dans le scénario de facturation spécifié	Écrire	bill-scenario*		
DeleteBillScenarioUsageModification	Accorde l'autorisation de supprimer l'utilisation nouvellement ajoutée dans le scénario de facturation spécifié	Écrire	bill-scenario*		
DeleteWorkloadEstimate	Accorde l'autorisation de supprimer l'estimation de charge de travail spécifiée	Écrire	workload-estimate*		
DeleteWorkloadEstimateUsage	Accorde l'autorisation de supprimer l'utilisation nouvellement ajoutée de l'estimation de charge de travail spécifiée	Écrire	workload-estimate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBillEstimate	Permet de récupérer les détails d'une estimation de facture, y compris le coût estimé	Lecture	bill-estimate*		
GetBillScenario	Accorde l'autorisation de récupérer les informations associées à un scénario de facturation	Lecture	bill-scenario*		
GetPreferences	Accorde l'autorisation de récupérer les préférences de type de taux applicables au compte	Lecture			
GetWorkloadEstimate	Accorde l'autorisation de récupérer les informations associées à une estimation de la charge de travail	Lecture	workload-estimate*		
ListBillEstimateCommitments	Permet de répertorier les engagements associés à l'estimation de facture spécifiée	List	bill-estimate*		
ListBillEstimateInputCommitmentModifications	Permet de répertorier les engagements ajoutés ou supprimés pour une estimation de facture spécifiée	List	bill-estimate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBillEstimateInputUsageModifications	Accorde l'autorisation de répertorier les utilisations ajoutées ou modifiées pour une estimation de facture spécifiée	List	bill-estimate*		
ListBillEstimateLineItems	Accorde l'autorisation de répertorier les éléments des lignes de résultat pour une estimation de facture spécifiée	List	bill-estimate*		
ListBillEstimates	Donne l'autorisation de répertorier les estimations de factures	List			
ListBillScenarioCommitmentModifications	Permet de répertorier les engagements inclus dans un scénario de facturation	List	bill-scenario*		
ListBillScenarioUsageModifications	Accorde l'autorisation de répertorier les lignes d'utilisation d'un scénario de facture spécifié	List	bill-scenario*		
ListBillScenarios	Accorde l'autorisation de répertorier les scénarios de facturation	List			
ListTagsForResource	Accorde l'autorisation de renvoyer une liste d'étiquettes pour une ressource	Identification			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWorkloadEstimateUsage	Accorde l'autorisation de répertorier les lignes d'utilisation pour l'estimation de charge de travail spécifiée	List	workload-estimate*		
ListWorkloadEstimates	Accorde l'autorisation de répertorier les estimations de charge de travail	List			
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource	Balisage	bill-scenario	aws:ResourceTag/${TagKey}	
			workload-estimate	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	bill-scenario	aws:ResourceTag/${TagKey}	
			workload-estimate	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateBillEstimate	Autorise la mise à jour de l'estimation de la facture, du nom et de la date d'expiration	Écrire	bill-estimate*		
UpdateBillScenario	Autorise la mise à jour du nom et de la date d'expiration du scénario de facture spécifié	Écrire	bill-scenario*		
UpdateBillScenarioCommitmentModification	Autorise la mise à jour du groupe d'engagements dans le scénario de facture spécifié	Écrire	bill-scenario*		
UpdateBillScenarioUsageModification	Accorde l'autorisation de mettre à jour le montant d'utilisation, l'heure d'utilisation et le groupe d'utilisation dans le scénario de facturation spécifié	Écrire	bill-scenario*		
UpdatePreferences	Accorde l'autorisation de mettre à jour les préférences de type de tarif pour le compte	Écrire			
UpdateWorkloadEstimate	Autorise la mise à jour du nom et de la date d'expiration de l'estimation de charge de travail spécifiée	Écrire	workload-estimate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateWorkloadEstimateUsage	Accorde l'autorisation de mettre à jour le montant d'utilisation et le groupe d'utilisation dans l'estimation de charge de travail spécifiée en fonction de l'identifiant d'utilisation	Écrire	workload-estimate*		

Types de ressources définis par AWS Billing And Cost Management Pricing Calculator

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
bill-estimate	`arn:${Partition}:bcm-pricing-calculator::${Account}:bill-estimate/${BillEstimateId}`	
bill-scenario	`arn:${Partition}:bcm-pricing-calculator::${Account}:bill-scenario/${BillScenarioId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
workload-estimate	`arn:${Partition}:bcm-pricing-calculator::${Account}:workload-estimate/${WorkloadEstimateId}`	aws:ResourceTag/${TagKey}

Clés de condition pour le calculateur de prix AWS Billing And Cost Management

AWS Billing Et le calculateur de prix de gestion des coûts définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les actions recommandées par AWS Billing And Cost Management

AWS Billing Et les actions recommandées pour la gestion des coûts (préfixe de service :`bcm-recommended-actions`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Billing et actions recommandées pour la gestion des coûts
- Types de ressources définis par AWS Billing And Cost Management Recommended Actions
- Clés de condition pour AWS Billing les actions recommandées et gestion des coûts

Actions définies par AWS Billing et actions recommandées pour la gestion des coûts

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRecommendedActions	Accorde l'autorisation de répertorier toutes les actions recommandées	List			

Types de ressources définis par AWS Billing And Cost Management Recommended Actions

AWS Billing Et les actions recommandées en matière de gestion des coûts ne permettent pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour

autoriser l'accès aux actions recommandées AWS Billing et à la gestion des coûts, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour AWS Billing les actions recommandées et gestion des coûts

BillingAndCostManagementRecommendedActions ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Billing Conductor

AWS Billing Conductor (préfixe de service :`billingconductor`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Billing Conductor
- Types de ressources définis par AWS Billing Conductor
- Clés de condition pour AWS Billing Conductor

Actions définies par AWS Billing Conductor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAccounts	Accorde l'autorisation d'associer entre un et 30 comptes à un groupe de facturation	Écrire	billinggroup*		
AssociatePricingRules	Accorde l'autorisation d'associer les règles de tarification	Écrire	pricingplan*		
			pricingrule*		
BatchAssociateResourcesToCustomLineItem	Accorde l'autorisation d'associer des ressources par lots à un élément de ligne personnalisé en pourcentage	Écrire	customlineitem*		
BatchDisassociateResourcesFromCustomLineItem	Accorde l'autorisation de dissocier des ressources par lots d'un élément de ligne personnalisé en pourcentage	Écrire	customlineitem*		
CreateBillingGroup	Accorde l'autorisation de créer un groupe de facturation	Écrire	pricingplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCustomLineItem	Accorde l'autorisation de créer un élément de ligne personnalisé	Écrire	billinggroup*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingPlan	Accorde l'autorisation de créer un plan de tarification	Écrire	pricingrule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingRule	Accorde l'autorisation de créer une règle de tarification	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBillingGroup	Accorde l'autorisation de supprimer un groupe de facturation	Écrire	billinggroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCustomLineItem	Accorde l'autorisation de supprimer un élément de ligne personnalisé	Écrire	customlineitem*		
DeletePricingPlan	Accorde l'autorisation de supprimer un plan de tarification	Écrire	pricingplan*		
DeletePricingRule	Accorde l'autorisation de supprimer une règle de tarification	Écrire	pricingrule*		
DisassociateAccounts	Accorde l'autorisation de détacher entre un et 30 comptes d'un groupe de facturation	Écrire	billinggroup*		
DisassociatePricingRules	Accorde l'autorisation de dissocier des règles de tarification	Écrire	pricingplan*		
			pricingrule*		
GetBillingGroupCostReport	Accorde l'autorisation d'afficher l'état des coûts du groupe de facturation pour un groupe de facturation spécifié	Lecture	billinggroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAccountAssociations	Accorde l'autorisation de répertorier les comptes liés du compte souscripteur pour la période de facturation donnée tout en fournissant le groupe de facturation auquel appartiennent les comptes liés	List			
ListBillingGroupCostReports	Accorde l'autorisation d'afficher l'état des coûts du groupe de facturation	Lecture			
ListBillingGroups	Accorde l'autorisation d’afficer les détails du groupe de facturation	Lecture			
ListCustomLineItemVersions	Accorde l'autorisation d'afficher les versions d'un élément de ligne personnalisé	Lecture	customlineitem*		
ListCustomLineItems	Accorde l'autorisation d’afficher les détails de l’élément de ligne personnalisé	Lecture			
ListPricingPlans	Accorde l'autorisation d'afficher les détails du plan de tarification	Lecture			
ListPricingPlansAssociatedWithPricingRule	Accorde l'autorisation de répertorier les plans de tarification associés à une règle de tarification	List	pricingrule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPricingRules	Accorde l'autorisation d'afficher les détails des règles de tarification	Lecture			
ListPricingRulesAssociatedToPricingPlan	Accorde l'autorisation de répertorier les règles de tarification associés à un plan de tarification	List	pricingplan*		
ListResourcesAssociatedToCustomLineItem	Accorde l'autorisation de répertorier des ressources à un élément de ligne personnalisé en pourcentage	List	customlineitem*		
ListTagsForResource	Accorde l'autorisation de répertorier les étiquettes d'une ressource	Lecture	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateBillingGroup	Accorde l'autorisation de mettre à jour un groupe de facturation	Écrire	billinggroup*		
UpdateCustomLineItem	Accorde l'autorisation de mettre à jour un élément de ligne personnalisé	Écrire	customlineitem*		
UpdatePricingPlan	Accorde l'autorisation de mettre à jour un plan de tarification	Écrire	pricingplan*		
UpdatePricingRule	Accorde l'autorisation de mettre à jour une règle de tarification	Écrire	pricingrule*		

Types de ressources définis par AWS Billing Conductor

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
billinggroup	`arn:${Partition}:billingconductor::${Account}:billinggroup/${BillingGroupId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
pricingplan	arn:${Partition}:billingconductor::${Account}:pricingplan/${PricingPlanId}	aws:ResourceTag/${TagKey}
pricingrule	arn:${Partition}:billingconductor::${Account}:pricingrule/${PricingRuleId}	aws:ResourceTag/${TagKey}
customlineitem	arn:${Partition}:billingconductor::${Account}:customlineitem/${CustomLineItemId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Billing Conductor

AWS Billing Conductor définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Billing la console

AWS Billing La console (préfixe de service :`aws-portal`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Billing la console
- Types de ressources définis par AWS Billing la console
- Clés de condition pour AWS Billing console

Actions définies par AWS Billing la console

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConsoleActionSetEnforced [autorisation uniquement]	Octroie l'autorisation de voir si des actions IAM existantes ou détaillées sont utilisées pour contrôler l'autorisation des consoles de facturation,	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	de gestion des coûts et de compte				
ModifyAccount [autorisation uniquement]	Permet d'accorder ou de refuser aux utilisateurs IAM l'autorisation de modifier les paramètres du compte	Écrire			
ModifyBilling [autorisation uniquement]	Permet d'accorder ou de refuser aux utilisateurs IAM l'autorisation de modifier les paramètres de facturation	Écrire			
ModifyPaymentMethods [autorisation uniquement]	Permet d'accorder ou de refuser aux utilisateurs IAM l'autorisation de modifier les modes de paiement	Écrire			
UpdateConsoleActionSetEnforced [autorisation uniquement]	Octroie l'autorisation de modifier l'utilisation ou non des actions IAM existantes ou détaillées pour contrôler l'autorisation des consoles de facturation, de gestion des coûts et de compte	Écrire			
ViewAccount [autorisation uniquement]	Permet d'accorder ou de refuser aux utilisateurs IAM l'autorisation d'afficher les paramètres du compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ViewBilling [autorisation uniquement]	Permet d'accorder ou de refuser aux utilisateurs IAM l'autorisation d'afficher les pages de facturation dans la console	Lecture			
ViewPaymentMethods [autorisation uniquement]	Permet d'accorder ou de refuser aux utilisateurs IAM l'autorisation d'afficher les modes de paiement	Lecture			
ViewUsage [autorisation uniquement]	Autoriser ou refuser aux utilisateurs IAM l'autorisation de consulter les rapports AWS d'utilisation	Lecture			

Types de ressources définis par AWS Billing la console

AWS Billing La console ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à la console AWS Billing , spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Billing console

La console de facturation ne dispose pas de clés de contexte spécifiques aux services pouvant être utilisées dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Braket

Amazon Braket (préfixe de service : `braket`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Braket
- Types de ressources définis par Amazon Braket
- Clés de condition pour Amazon Braket

Actions définies par Amazon Braket

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptUserAgreement [autorisation uniquement]	Accorde l'autorisation d'accepter l'accord d'utilisation d'Amazon Braket	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelJob	Accorde l'autorisation d'annuler une tâche	Écrire	job*		
CancelQuantumTask	Accorde l'autorisation d'annuler une tâche quantique	Écrire	quantum-task*		
CreateJob	Accorde l'autorisation de créer une tâche.	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateQuantumTask	Accorde l'autorisation de créer une tâche quantique	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSpendingLimit	Autorise la création d'une limite de dépenses	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteSpendingLimit	Autorise la suppression d'une limite de dépenses	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
GetDevice	Accorde l'autorisation de récupérer des informations sur les appareils disponibles dans Amazon Braket	Lecture			
GetJob	Accorde l'autorisation de récupérer des tâches	Lecture	job*		
GetQuantumTask	Accorde l'autorisation de récupérer des tâches quantiques	Lecture	quantum-task*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceLinkedRoleStatus [autorisation uniquement]	Accorde l'autorisation de vérifier si le rôle lié au service Amazon Braket a été créé	Lecture			
GetUserAgreementStatus [autorisation uniquement]	Accorde l'autorisation de vérifier si le compte a accepté l'accord d'utilisation d'Amazon Braket	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises qui ont été appliquées à la ressource de tâche quantique ou à la tâche	Lecture	job		
			quantum-task		
			spending-limit		
SearchDevices	Accorde l'autorisation de rechercher les appareils disponibles dans Amazon Braket	Lecture			
SearchJobs	Accorde l'autorisation de rechercher des tâches	Lecture			
SearchQuantumTasks	Accorde l'autorisation de rechercher des tâches quantiques	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchSpendingLimits	Autorise la recherche d'une limite de dépenses	Lecture			
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une tâche quantique ou à un travail hybride	Identification	job		
			quantum-task		
			spending-limit		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource de tâche quantique ou d'une tâche Une balise est constitué e d'une paire clé-valeur	Identification	job		
			quantum-task		
			spending-limit		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSpendingLimit	Autorise la mise à jour d'une limite de dépenses	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Types de ressources définis par Amazon Braket

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
quantum-task	`arn:${Partition}:braket:${Region}:${Account}:quantum-task/${RandomId}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:braket:${Region}:${Account}:job/${JobName}`	aws:ResourceTag/${TagKey}
spending-limit	`arn:${Partition}:braket:${Region}:${Account}:spending-limit/${RandomId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Braket

Amazon Braket définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Budget Service

AWS Budget Service (préfixe de service :`budgets`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Budget Service
- Types de ressources définis par AWS Budget Service
- Clés de condition pour AWS Budget Service

Actions définies par AWS Budget Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> Les actions indiquées dans ce tableau ne le sont pas APIs, mais sont plutôt des autorisations qui accordent l' AWS Billing and Cost Management APIs accès aux budgets correspondants.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBudgetAction	Accorde l'autorisation de configurer une réponse qui s'exécute une fois que votre budget dépasse un seuil budgétaire spécifique. La création d'une action budgétaire avec des balises nécessite également l'autorisation « budgets : TagResource »	Écrire	budgetAction*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteBudgetAction	Accorde l'autorisation de supprimer une action associée à un budget spécifique	Écrire	budgetAction*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeBudgetAction	Accorde l'autorisation de récupérer les détails d'une action budgétaire spécifique associée à un budget	Lecture	budgetAction*		
DescribeBudgetActionHistories	Accorde l'autorisation de récupérer une vue historique des statuts des actions budgétaires associés à une action budgétaire particulière. Ces statuts peuvent être « Standby », « Pending » et « Executed »	Lecture	budgetAction*		
DescribeBudgetActionsForAccount	Accorde l'autorisation de récupérer les détails de toutes les actions budgétaires associées à votre compte	Lecture			
DescribeBudgetActionsForBudget	Accorde l'autorisation de récupérer les détails de toutes les actions budgétaires associées à un budget	Lecture	budget*		
ExecuteBudgetAction	Accorde l'autorisation de lancer une action budgétaire en attente et d'annuler une action budgétaire précédemment exécutée	Écrire	budgetAction*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation d'afficher les balises de ressources pour un budget ou une action budgétaire	Lecture	budget		
			budgetAction		
ModifyBudget	Accorde l'autorisation de créer et de modifier des budgets, ainsi que de modifier les détails du budget. La création d'un budget avec des balises nécessite également l'autorisation « budgets : TagResource »	Écrire	budget*		iam:CreateServiceLinkedRole
TagResource	Accorde l'autorisation d'appliquer des balises de ressources à un budget ou à une action budgétaire. Également nécessaire pour créer un budget ou une action budgétaire avec des balises	Identification	budget		
			budgetAction		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les balises de ressources d'un budget ou d'une action budgétaire	Identification	budget		
			budgetAction		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateBudgetAction	Accorde l'autorisation de mettre à jour les détails d'une action budgétaire spécifique associée à un budget	Écrire	budgetAction*		iam:PassRole
ViewBudget	Accorde l'autorisation d'afficher les budgets et les détails budgétaires	Lecture	budget*		billing:GetBillingViewData

Types de ressources définis par AWS Budget Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
budget	`arn:${Partition}:budgets::${Account}:budget/${BudgetName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Types de ressources	ARN	Clés de condition
budgetAction	`arn:${Partition}:budgets::${Account}:budget/${BudgetName}/action/${ActionId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Clés de condition pour AWS Budget Service

AWS Budget Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS BugBust

AWS BugBust (préfixe de service :`bugbust`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS BugBust
- Types de ressources définis par AWS BugBust
- Clés de condition pour AWS BugBust

Actions définies par AWS BugBust

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEvent [autorisation uniquement]	Accorde l'autorisation de créer un BugBust événement	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
EvaluateProfilingGroups	Accorde l'autorisation d'évaluer des groupes de profilage archivés	Écriture	Event*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
GetEvent [autorisation uniquement]	Accorde l'autorisation d'afficher les informations clients sur un événement	Lecture	Event*		
				aws:ResourceTag/${TagKey}	
GetJoinEventStatus [autorisation uniquement]	Permet de consulter le statut de la tentative d'un BugBust joueur de participer à un BugBust événement	Lecture	Event*		
				aws:ResourceTag/${TagKey}	
JoinEvent [autorisation uniquement]	Accorde l'autorisation de rejoindre un événement	Écriture	Event*		
				aws:ResourceTag/${TagKey}	
ListBugs [autorisation uniquement]	Accorde l'autorisation d'afficher les bogues importés dans un événement pour que les joueurs puissent travailler dessus	Lecture	Event*		codeguru-reviewer:DescribeCodeReview codeguru-reviewer:ListRecommendations

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ListEventParticipants [autorisation uniquement]	Accorde l'autorisation d'afficher les participants d'un événement	Lecture	Event*		
				aws:ResourceTag/${TagKey}	
ListEventScores [autorisation uniquement]	Accorde l'autorisation d'afficher les scores des joueurs d'un événement	Lecture	Event*		
				aws:ResourceTag/${TagKey}	
ListEvents [autorisation uniquement]	Accorde l'autorisation de répertorier BugBust les événements	List		aws:ResourceTag/${TagKey}	
ListProfilingGroups [autorisation uniquement]	Accorde l'autorisation d'afficher les groupes de profilage importés dans un événement pour que les joueurs puissent travailler dessus	Lecture	Event*		
				aws:ResourceTag/${TagKey}	
ListPullRequests [autorisation uniquement]	Accorde l'autorisation d'afficher les demandes d'extraction utilisées par les joueurs pour soumettre des correctifs aux bogues identifiés lors d'un événement	Lecture	Event*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation de répertorier les balises pour une ressource Bugbust.	Lecture	Event*		
				aws:ResourceTag/${TagKey}	
TagResource [autorisation uniquement]	Accorde l'autorisation de baliser une ressource Bugbust	Balisage	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation d'annuler le balisage d'une ressource Bugbust	Balisage	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEvent [autorisation uniquement]	Autorise la mise à jour d'un BugBust événement	Écrire	Event*		codeguru-profiler: DescribeProfilingGroup codeguru-profiler: ListProfilingGroups codeguru-reviewer: DescribeCodeReview codeguru-reviewer: ListCodeReviews codeguru-reviewer: ListRecommendations codeguru-reviewer: TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					codeguru-reviewer: UnTagResource
				aws:ResourceTag/${TagKey}	
UpdateWorkItem [autorisation uniquement]	Accorde l'autorisation de mettre à jour un élément de travail comme identifié ou non identifié (bogue ou groupe de profilage)	Écriture	Event*		codeguru-reviewer: ListRecommendations
				aws:ResourceTag/${TagKey}	
UpdateWorkItemAdmin [autorisation uniquement]	Accorde l'autorisation de mettre à jour l'élément de travail d'un événement (bogue ou groupe de profilage)	Écrire	Event*		codeguru-reviewer: ListRecommendations
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS BugBust

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Event	`arn:${Partition}:bugbust:${Region}:${Account}:events/${EventId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS BugBust

AWS BugBust définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Certificate Manager

AWS Certificate Manager (préfixe de service :`acm`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Certificate Manager
- Types de ressources définis par AWS Certificate Manager
- Clés de condition pour AWS Certificate Manager

Actions définies par AWS Certificate Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTagsToCertificate	Accorde l'autorisation d'ajouter une ou plusieurs balises à un certificat	Balisage	certificate*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DeleteCertificate	Accorde l'autorisation de supprimer un certificat et la clé privée associée	Écriture	certificate*		
DescribeCertificate	Accorde l'autorisation de récupérer un certificat et ses métadonnées	Lecture	certificate*		
ExportCertificate	Autorise l'exportation d'un certificat exportable pour une utilisation en tout lieu	Lecture	certificate*		
				acm:DomainNames	
GetAccountConfiguration	Accorde l'autorisation de récupérer la configuration au niveau du compte depuis AWS Certificate Manager	Lecture			
GetCertificate	Accorde l'autorisation de récupérer un certificat et une chaîne de certificats pour un ARN de certificat	Lecture	certificate*		
ImportCertificate	Autorise l'importation d'un certificat tiers dans AWS Certificate Manager (ACM)	Écrire	certificate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCertificates	Accorde l'autorisation de récupérer une liste de certificats pour des paramètres de certificat spécifiques	List			
ListTagsForCertificate	Accorde l'autorisation de répertorier les balises associées à un certificat	Lecture	certificate*		
PutAccountConfiguration	Accorde l'autorisation de mettre à jour la configuration au niveau du compte dans AWS Certificate Manager	Écrire			
RemoveTagsFromCertificate	Accorde l'autorisation de supprimer une ou plusieurs balises d'un certificat	Balisage	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RenewCertificate	Accorde l'autorisation de renouveler un certificat privé admissible	Écriture	certificate*		
RequestCertificate	Accorde l'autorisation de demander un certificat public ou privé	Écriture		aws:RequestTag/${TagKey} aws:TagKeys acm:DomainNames acm:CertificateTransparencyLogging acm:ValidationMethod acm:KeyAlgorithm acm:CertificateAuthority acm:Export	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResendValidationEmail	Accorde l'autorisation de renvoyer un e-mail pour demander la validation de la propriété du domaine	Écrire	certificate*		
RevokeCertificate	Accorde l'autorisation de révoquer un certificat exportable	Écrire	certificate*		
				acm:DomainNames	
SearchCertificates	Accorde l'autorisation de récupérer une liste de certificats correspondant aux critères de recherche	List			
UpdateCertificateOptions	Accorde l'autorisation de mettre à jour la configuration d'un certificat. Permet de spécifier s'il faut choisir ou pas la journalisation de la transparence des certificats	Écrire	certificate*		

Types de ressources définis par AWS Certificate Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
certificate	`arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Certificate Manager

AWS Certificate Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
acm:CertificateAuthority	Filtre l'accès en fonction de certificateAuthority dans la requête. Peut être utilisé pour restreindre les autorités de certification à partir desquelles les certificats peuvent être émis	String
acm:CertificateTransparencyLogging	Filtre l'accès par certificateTransparencyLogging option dans la demande. Par défaut, « ACTIVÉ » si aucune clé n'est présente dans la requête	String
acm:DomainNames	Filtre l'accès par domainNames dans la requête. Cette clé peut être utilisée pour restreindre les domaines pouvant figurer dans les requêtes de certificat	ArrayOfString
acm:Export	Filtre l'accès par l'option d'exportation figurant dans la demande. Peut être utilisé pour restreindre la création de certificats pouvant être exportés	String

Clés de condition	Description	Type
acm:KeyAlgorithm	Filtre l'accès en fonction de keyAlgorithm dans la requête	String
acm:ValidationMethod	Filtre l'accès en fonction de validationMethod dans la requête. Par défaut, « E-MAIL » si aucune clé n'est présente dans la requête	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Chatbot

AWS Chatbot (préfixe de service :`chatbot`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Chatbot
- Types de ressources définis par AWS Chatbot
- Clés de condition pour AWS Chatbot

Actions définies par AWS Chatbot

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateToConfiguration	Accorde l'autorisation d'associer une ressource à une configuration	Écrire	ChatbotConfiguration*		
			custom-action*		
				aws:ResourceTag/${TagKey}	
CreateChimeWebhookConfiguration	Accorde l'autorisation de créer une configuration AWS Chatbot Chime Webhook	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomAction	Accorde l'autorisation de créer une action personnalisée	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMicrosoftTeamsChannelConfiguration	Accorde l'autorisation de créer une configuration de canal AWS Microsoft Teams pour chatbot	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSlackChannelConfiguration	Accorde l'autorisation de créer une configuration de canal Slack pour AWS Chatbot	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChimeWebhookConfiguration	Autorise la suppression d'une configuration de AWS chatbot Chime Webhook	Écrire	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteCustomAction	Accorde l'autorisation de supprimer une action personnalisée	Écrire	custom-action*		
				aws:ResourceTag/${TagKey}	
DeleteMicrosoftTeamsChannelConfiguration	Accorde l'autorisation de supprimer la configuration d'un AWS canal Microsoft Teams d'un Chatbot	Écrire	ChatbotConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteMicrosoftTeamsConfiguredTeam	Accorde l'autorisation de supprimer les Microsoft Teams configurées avec AWS Chatbot dans un Compte AWS	Écrire			
DeleteMicrosoftTeamsUserIdentity	Accorde l'autorisation de supprimer l'identité d' AWS utilisateur Microsoft Teams d'un Chatbot	Écrire			
DeleteSlackChannelConfiguration	Accorde l'autorisation de supprimer la configuration du canal AWS Slack d'un Chatbot	Écrire	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteSlackUserIdentity	Accorde l'autorisation de supprimer l'identité d'utilisateur AWS Slack d'un Chatbot	Écrire			
DeleteSlackWorkspaceAuthorization	Accorde l'autorisation de supprimer l'autorisation de l'espace de travail Slack avec AWS Chatbot, associée à un Compte AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeChimeWebhookConfigurations	Permet de répertorier toutes les configurations de AWS Chatbot Chime Webhook dans un compte AWS	Lecture			
DescribeSlackChannelConfigurations	Permet de répertorier toutes les configurations du canal Slack du AWS Chatbot dans un Compte AWS	Lecture			
DescribeSlackChannels	Permet de répertorier toutes les chaînes Slack publiques de l'espace de travail Slack connectées au AWS compte intégré au service Chatbot AWS	Lecture			
DescribeSlackUserIdentities	Accorde l'autorisation de décrire les identités des utilisateurs de AWS Chatbot Slack	Lecture			
DescribeSlackWorkspaces	Permet de répertorier tous les espaces de travail Slack autorisés connectés au AWS compte intégré au service Chatbot AWS	Lecture			
DisassociateFromConfiguration	Accorde l'autorisation de dissocier une ressource d'une configuration	Écrire	ChatbotConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			custom-action*		
				aws:ResourceTag/${TagKey}	
GetAccountPreferences	Accorde l'autorisation de récupérer les préférences du AWS compte Chatbot	Lecture			
GetCustomAction	Accorde l'autorisation d'effectuer une action personnalisée	Lecture	custom-action*		
				aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsChannelConfiguration	Accorde l'autorisation d'obtenir un seul AWS Chatbot Microsoft Teams Channel Configurations dans un Compte AWS	Lecture		aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsOauthParameters	Accorde l'autorisation de générer des OAuth paramètres pour demander le OAuth code Microsoft Teams à utiliser par le service AWS Chatbot	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSlackOauthParameters	Accorde l'autorisation de générer des OAuth paramètres pour demander le OAuth code Slack à utiliser par le service AWS Chatbot	Lecture			
ListAssociations	Accorde l'autorisation de répertorier les ressources associées à une configuration	Lecture	ChatbotConfiguration*		
ListCustomActions	Accorde l'autorisation de répertorier les actions personnalisées	List			
ListMicrosoftTeamsChannelConfigurations	Accorde l'autorisation de répertorier toutes les configurations de canaux AWS Microsoft Teams de Chatbot dans un Compte AWS	Lecture			
ListMicrosoftTeamsConfiguredTeams	Accorde l'autorisation de répertorier toutes les équipes Microsoft connectées au AWS compte intégré au service Chatbot AWS	Lecture			
ListMicrosoftTeamsUserIdentities	Accorde l'autorisation de décrire les identités des utilisateurs du AWS Chatbot Microsoft Teams	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier tous les tags associés à la configuration du AWS canal Chatbot	Lecture			
RedeemMicrosoftTeamsOauthCode	Accorde l'autorisation de racheter les paramètres précédemment générés auprès de Microsoft APIs, afin d'acquérir OAuth des jetons à utiliser par le service AWS Chatbot	Écrire			
RedeemSlackOauthCode	Accorde l'autorisation d'utiliser les paramètres précédemment générés avec l'API Slack, afin d'acquérir OAuth des jetons à utiliser par le service Chatbot AWS	Écrire			
TagResource	Accorde l'autorisation de créer des tags sur la configuration du AWS canal Chatbot	Identification	ChatbotConfiguration		
			custom-action		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des tags sur la configuration du AWS canal Chatbot	Identification	ChatbotConfiguration		
			custom-action		
				aws:TagKeys	
UpdateAccountPreferences	Autorise la mise à jour des préférences du AWS compte Chatbot	Écrire			
UpdateChimeWebhookConfiguration	Accorde l'autorisation de mettre à jour la configuration d'un AWS chatbot Chime Webhook	Écrire	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateCustomAction	Accorde l'autorisation de mettre à jour une action personnalisée	Écrire	custom-action*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateMicrosoftTeamsChannelConfiguration	Accorde l'autorisation de mettre à jour la configuration d'un AWS canal Microsoft Teams d'un Chatbot	Écrire	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateSlackChannelConfiguration	Accorde l'autorisation de mettre à jour la configuration du canal Slack d'un AWS Chatbot	Écrire	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS Chatbot

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
ChatbotConfiguration	`arn:${Partition}:chatbot::${Account}:chat-configuration/${ConfigurationType}/${ChatbotConfigurationName}`	aws:ResourceTag/${TagKey}
custom-action	`arn:${Partition}:chatbot::${Account}:custom-action/${ActionName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Chatbot

AWS Chatbot définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Chime

Amazon Chime (préfixe de service : `chime`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Chime
- Types de ressources définis par Amazon Chime
- Clés de condition pour Amazon Chime

Actions définies par Amazon Chime

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptDelegate	Accorde l'autorisation d'accepter l'invitation du délégué à partager la gestion d'un compte Amazon Chime avec un autre compte AWS	Écrire			
ActivateUsers	Accorde l'autorisation d'activer des utilisateurs dans un compte Amazon Chime de type entreprise	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddDomain	Accorde l'autorisation d'ajouter un domaine à votre compte Amazon Chime	Écriture			
AddOrUpdateGroups	Accorde l'autorisation d'ajouter de nouveaux groupes d'utilisateurs ou de mettre à jour des groupes existants Active Directory ou Okta associés à votre compte Amazon Chime de type entreprise	Écrire			
AssociateChannelFlow	Accorde l'autorisation d'associer un flux à un canal	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		
AssociatePhoneNumberWithUser	Accorde l'autorisation d'associer un numéro de téléphone à un utilisateur Amazon Chime	Écriture			
AssociatePhoneNumbersWithVoiceConnector	Accorde l'autorisation d'associer plusieurs numéros de téléphone à un Amazon Chime Voice Connector	Écriture	voice-connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociatePhoneNumbersWithVoiceConnectorGroup	Accorde l'autorisation d'associer plusieurs numéros de téléphone à un groupe de Amazon Chime Voice Connector	Écrire			
AssociateSigninDelegateGroupsWithAccount	Accorde l'autorisation d'associer les groupes de délégués de connexion spécifiés au compte Amazon Chime spécifié	Écrire			
AssociateVoiceConnectorConnect [autorisation uniquement]	Accorde l'autorisation d'associer l'instance Amazon Connect spécifiée à un Amazon Chime Voice Connector	Écrire			
AuthorizeDirectory	Accorde l'autorisation d'approuver un répertoire Active Directory pour votre compte Amazon Chime de type entreprise	Écriture			
BatchCreateAttendee	Accorde l'autorisation de créer de nouveaux participants pour une réunion active du kit SDK d'Amazon Chime	Écrire	meeting*		
BatchCreateChannelMembership	Octroie l'autorisation d'ajouter plusieurs utilisateurs et bots à un canal	Écrire	app-instance-bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			app-instance-user*		
			channel*		
BatchCreateRoomMembership	Accorde l'autorisation d'ajouter par lots des membres de la salle	Écriture			
BatchDeletePhoneNumber	Accorde l'autorisation de transférer 50 numéros de téléphone maximum à la file d'attente de suppression	Écriture			
BatchSuspendUser	Accorde l'autorisation de suspendre 50 utilisateurs maximum à partir d'un compte Amazon Chime de type équipe ou entrepriseLWA.	Écriture			
BatchUnsuspendUser	Accorde l'autorisation de lever la suspension de 50 utilisateurs maximum précédemment suspendus pour le compte Amazon Chime de type enterpriseLWA spécifié.	Écrire			
BatchUpdateAttendeeCapabilitiesExcept	Accorde l'autorisation de mise à jour AttendeeCapabilities , à l'exception des fonctionnalités répertoriées dans un ExcludedAttendeeIds tableau	Écrire	meeting*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdatePhoneNumber	Permet de mettre à jour les détails des numéros de téléphone dans l' UpdatePhoneNumberRequestItem objet pour un maximum de 50 numéros de téléphone	Écrire			
BatchUpdateUser	Accorde l'autorisation de mettre à jour les informations utilisateur au sein de l' UpdateUserRequestItem objet pour un maximum de 20 utilisateurs pour le compte Amazon Chime spécifié	Écrire			
ChannelFlowCallback	Accorde l'autorisation de rappeler un message sur un canal	Écrire	channel*		
Connect	Accorde l'autorisation d'établir une connexion WebSocket pour l'utilisateur de l'instance d'application au point de terminaison de la session de messagerie	Écriture	app-instance-user*		
ConnectDirectory	Accorde l'autorisation de connecter un répertoire Active Directory à votre compte Amazon Chime de type entreprise	Écrire			ds:ConnectDirectory

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAccount	Accorde l'autorisation de créer un compte Amazon Chime auprès de l'administrateur Compte AWS	Écrire			
CreateApiKey	Accorde l'autorisation de créer une nouvelle clé d'accès SCIM pour votre compte Amazon Chime et votre configuration Okta	Écrire			
CreateAppInstance	Accorde l'autorisation de créer une instance d'application dans le Compte AWS (les contrôles d'accès basés sur des balises ne sont pris en charge que sur identity-chime). (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceAdmin	Accorde l'autorisation de promouvoir un utilisateur ou un bot au rang de AppInstanceAdmin	Écrire	app-instance*		
			app-instance-bot*		
			app-instance-user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAppInstanceBot	Accorde l'autorisation de créer un bot dans un AppInstance (les contrôles d'accès basés sur des balises) ne sont pris en charge que sur identity-chime. (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceUser	Accorde l'autorisation de créer un utilisateur au sein d'un AppInstance (les contrôles d'accès basés sur des balises) ne sont pris en charge que sur identity-chime. (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAttendee	Accorde l'autorisation de créer un nouveau participant pour une réunion active du kit SDK d'Amazon Chime	Écriture	meeting*		
CreateBot	Accorde l'autorisation de créer un bot pour un compte Amazon Chime de type entreprise	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCDRBucket	Accorde l'autorisation de créer un nouveau compartiment Call Detail Record S3	Écrire			s3:CreateBucket s3:ListAllMyBuckets
CreateChannel	Accorde l'autorisation de créer un canal pour une instance d'application dans le Compte AWS (les contrôles d'accès basés sur des balises ne sont pris en charge que sur Messaging-Chime). (points de <region>terminaison .amazonaws.com)	Écrire	app-instance-bot*		
			app-instance-user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelBan	Octroie l'autorisation d'exclure un utilisateur ou un bot d'une chaîne	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateChannelFlow	Accorde l'autorisation de créer un flux de canaux pour une instance d'application dans le Compte AWS (les contrôles d'accès basés sur des balises ne sont pris en charge que sur Messaging-Chime). (points de <region>terminaison .amazonaws.com)	Écrire	app-instance*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelMembership	Octroie l'autorisation d'ajouter un utilisateur ou un bot à une chaîne	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateChannelModerator	Accorde l'autorisation de créer un modérateur de chaîne.	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConnectAnalyticsConnector [autorisation uniquement]	Accorde l'autorisation de créer un connecteur Amazon Connect Analytics dans le Compte AWS (les contrôles d'accès basés sur des balises ne sont pris en charge que sur le carillon vocal). (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateConnectCallTransferConnector [autorisation uniquement]	Accorde l'autorisation de créer un connecteur de transfert d'appels Amazon Connect dans le Compte AWS (les contrôles d'accès basés sur des balises ne sont pris en charge que sur le carillon vocal). (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateMediaCapturePipeline	Accorde l'autorisation de créer un pipeline de capture multimédia (les contrôles d'accès basés sur des balises ne sont pris en charge que sur media-pipelines-chime. (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMediaConcatenationPipeline	Accorde l'autorisation de créer un pipeline de concaténation multimédia (les contrôles d'accès basés sur des balises ne sont pris en charge que sur. media-pipelines-chime (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaInsightsPipeline	Accorde l'autorisation de créer un pipeline d'informations sur les médias (les contrôles d'accès basés sur des balises ne sont pris en charge que sur media-pipelines-chime. (points de <region>terminaison .amazonaws.com)	Écrire	media-insights-pipeline-configuration*		chime:TagResource kinesisvideo:DescribeStream
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMediaInsightsPipelineConfiguration	Accorde l'autorisation de créer une configuration de pipeline Media Insights (les contrôles d'accès basés sur des balises ne sont pris en charge que sur media-pipelines-chime.(points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource iam:PassRole kinesis:DescribeStream s3:ListBucket
CreateMediaLiveConnectorPipeline	Accorde l'autorisation de créer un pipeline Media Live Connector (les contrôles d'accès basés sur des balises ne sont pris en charge que sur media-pipelines-chime.(points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMediaPipelineKinesisVideoStreamPool	Accorde l'autorisation de créer un pool de flux vidéo Kinesis (les contrôles d'accès basés sur des balises ne sont pris en charge que sur. media-pipelines-chime (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	kinesis:DescribeStream kinesisvideo:CreateStream kinesisvideo:GetDataEndpoint kinesisvideo:ListStreams
CreateMediaStreamPipeline	Accorde l'autorisation de créer un pipeline de flux multimédia (les contrôles d'accès basés sur des balises ne sont pris en charge que sur media-pipelines-chime. (points de <region>terminaison .amazonaws.com)	Écrire	media-pipeline-kinesis-video-stream-pool*		kinesisvideo:DescribeStream kinesisvideo:GetDataEndpoint kinesisvideo:PutMedia

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMeeting	Accorde l'autorisation de créer une nouvelle réunion dans la région multimédia spécifiée, sans aucun participant initial (les contrôles d'accès basés sur des balises ne sont pris en charge que sur meetings-chime). (points de <region>terminaison .amazonaws.com)	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMeetingDialOut	Accorde l'autorisation d'appeler un numéro de téléphone pour rejoindre la réunion SDK Amazon Chime spécifiée.	Écrire	meeting*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMeetingWithAttendees	Accorde l'autorisation de créer une nouvelle réunion dans la région multimédia spécifiée, avec un ensemble de participants (les contrôles d'accès basés sur des balises ne sont pris en charge que sur meetings-chime). (points de <region>terminaison .amazonaws.com)	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePhoneNumberOrder	Accorde l'autorisation de créer une commande de numéros de téléphone avec les opérateurs	Écriture			
CreateProxySession	Accorde l'autorisation de créer une session proxy pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
CreateRoom	Accorde l'autorisation de créer une salle	Écriture			
CreateRoomMembership	Accorde l'autorisation d'ajouter un membre à la salle	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSipMediaApplication	Accorde l'autorisation de créer une application multimédia SIP Amazon Chime dans le Compte AWS (les contrôles d'accès basés sur des balises ne sont pris en charge que sur Voice-Chime). (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSipMediaApplicationCall	Accorde l'autorisation de créer un appel sortant pour l'application multimédia Amazon Chime SIP sous le Compte AWS	Écrire	sip-media-application*		
CreateSipRule	Accorde l'autorisation de créer une règle SIP Amazon Chime sous le Compte AWS	Écrire	sip-media-application		
CreateUser	Accorde l'autorisation de créer un utilisateur sous le compte Amazon Chime spécifié	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateVoiceConnector	Accorde l'autorisation de créer un connecteur vocal dans le Compte AWS (les contrôles d'accès basés sur des balises ne sont pris en charge que sur le carillon vocal). (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateConnectAnalyticsConnector chime:CreateConnectCallTransferConnector
CreateVoiceConnectorGroup	Accorde l'autorisation de créer un groupe de connecteurs vocaux Amazon Chime sous le nom de l'administrateur Compte AWS	Écrire	voice-connector		
CreateVoiceProfile	Octroie l'autorisation de créer un profil vocal	Écrire			
CreateVoiceProfileDomain	Accorde l'autorisation de créer un domaine de profil vocal (les contrôles d'accès basés sur des balises ne sont pris en charge que sur les carillons vocaux). (points de <region>terminaison .amazonaws.com)	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource kms:CreateGrant kms:DescribeKey

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccount	Accorde l'autorisation de supprimer le compte Amazon Chime spécifié	Écrire			
DeleteAccountOpenIdConfig	Accorde l'autorisation de supprimer les OpenIdConfig attributs de votre compte Amazon Chime	Écrire			
DeleteApiKey	Accorde l'autorisation de supprimer la clé d'accès SCIM associée à votre compte Amazon Chime et à votre configuration Okta	Écrire			
DeleteAppInstance	Accorde l'autorisation de supprimer un AppInstance	Écrire	app-instance*		
DeleteAppInstanceAdmin	Accorde l'autorisation de AppInstanceAdmin rétrograder un utilisateur ou un robot	Écrire	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DeleteAppInstanceBot	Accorde l'autorisation de supprimer un AppInstanceBot	Écrire	app-instance-bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAppInstanceStreamingConfigurations	Accorde l'autorisation de désactiver le streaming de données pour l'instance d'application.	Écrire	app-instance*		
DeleteAppInstanceUser	Accorde l'autorisation de supprimer un AppInstanceUser	Écrire	app-instance-user*		
DeleteAttendee	Accorde l'autorisation de supprimer le participant spécifié d'une réunion du kit SDK d'Amazon Chime	Écriture	meeting*		
DeleteCDRBucket	Accorde l'autorisation de supprimer un compartiment Call Detail Record S3 à partir de votre compte Amazon Chime	Écriture			s3:DeleteBucket
DeleteChannel	Accorde l'autorisation de supprimer un canal.	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelBan	Octroie l'autorisation de supprimer un utilisateur ou un bot de la liste d'exclusion d'un canal	Écrire	app-instance-bot*		
			app-instance-user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			channel*		
DeleteChannelFlow	Accorde l'autorisation de supprimer un flux de canal	Écrire	channel*		
DeleteChannelMembership	Accorde l'autorisation de supprimer un membre d'une chaîne.	Écriture	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelMessage	Accorde l'autorisation de supprimer un message de chaîne.	Écriture	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelModerator	Accorde l'autorisation de supprimer un modérateur de chaîne.	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteDelegate	Autorise la suppression de Compte AWS la gestion déléguée de votre compte Amazon Chime	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDomain	Accorde l'autorisation de supprimer un domaine de votre compte Amazon Chime	Écriture			
DeleteEventsConfiguration	Accorde l'autorisation de supprimer les détails de configuration d'événements pour qu'un bot puisse recevoir les événements sortants	Écriture			
DeleteGroups	Accorde l'autorisation de supprimer des groupes d'utilisateurs Active Directory ou Okta de votre compte Amazon Chime de type entreprise	Écriture			
DeleteMediaCapturePipeline	Accorde l'autorisation de supprimer un pipeline de capture du média	Écrire	media-pipeline*		
DeleteMediaInsightsPipelineConfiguration	Octroie l'autorisation de supprimer une configuration de pipeline d'informations multimédias	Écrire	media-insights-pipeline-configuration*		chime:ListVoiceConnectors
DeleteMediaPipeline	Accorde l'autorisation de supprimer un pipeline du média	Écrire	media-pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteMediaPipelineKinesisVideoStreamPool	Accorde l'autorisation de supprimer un groupe de flux vidéo Kinesis.	Écrire	media-pipeline-kinesis-video-stream-pool*		
DeleteMeeting	Accorde l'autorisation de supprimer la réunion spécifiée du kit SDK d'Amazon Chime	Écrire	meeting*		
DeleteMessagingStreamingConfigurations	Accorde l'autorisation de supprimer les configurations de diffusion de données d'un AppInstance	Écrire	app-instance*		
DeletePhoneNumber	Accorde l'autorisation de transférer un numéro de téléphone à la file d'attente de suppression	Écriture			
DeleteProxySession	Accorde l'autorisation de supprimer une session proxy pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
DeleteRoom	Accorde l'autorisation de supprimer une salle	Écriture			
DeleteRoomMembership	Accorde l'autorisation de supprimer un membre de la salle	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSipMediaApplication	Autorise l'administrateur à supprimer l'application multimédia Amazon Chime SIP Compte AWS	Écrire	sip-media-application*		
DeleteSipRule	Accorde l'autorisation de supprimer la règle SIP Amazon Chime sous le nom de l'administrateur Compte AWS	Écrire			
DeleteVoiceConnector	Accorde l'autorisation de supprimer le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
DeleteVoiceConnectorEmergencyCallingConfiguration	Accorde l'autorisation de supprimer la configuration des appels d'urgence pour le Amazon Chime Voice Connector spécifié	Écrire	voice-connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteVoiceConnectorExternalSystemsConfiguration	Accorde l'autorisation de supprimer la configuration du système externe connecté au connecteur vocal Amazon Chime spécifié	Écrire	voice-connector*		
DeleteVoiceConnectorGroup	Accorde l'autorisation de supprimer le groupe de Amazon Chime Voice Connector spécifié	Écriture			
DeleteVoiceConnectorOrigination	Accorde l'autorisation de supprimer les paramètres d'origine pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
DeleteVoiceConnectorProxy	Accorde l'autorisation de supprimer la configuration du proxy pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
DeleteVoiceConnectorStreamingConfiguration	Accorde l'autorisation de supprimer la configuration du streaming pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteVoiceConnectorTermination	Accorde l'autorisation de supprimer les paramètres de résiliation pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
DeleteVoiceConnectorTerminationCredentials	Accorde l'autorisation de supprimer les informations d'identification de résiliation SIP pour le Amazon Chime Voice Connector spécifié	Écrire	voice-connector*		
DeleteVoiceProfile	Octroie l'autorisation de supprimer un profil vocal	Écrire	voice-profile*		
DeleteVoiceProfileDomain	Octroie l'autorisation de supprimer un domaine de profil vocal	Écrire	voice-profile-domain*		
DeregisterAppInstanceUserEndpoint	Accorde l'autorisation d'annuler l'enregistrement d'un point de terminaison pour un utilisateur d'instance d'application	Écrire	app-instance-user*		
DescribeAppInstance	Accorde l'autorisation d'obtenir tous les détails d'un AppInstance	Lecture	app-instance*		
DescribeAppInstanceAdmin	Accorde l'autorisation d'obtenir tous les détails d'un AppInstanceAdmin	Lecture	app-instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			app-instance-bot*		
			app-instance-user*		
DescribeAppInstanceBot	Accorde l'autorisation d'obtenir tous les détails d'un AppInstanceBot	Lecture	app-instance-bot*		
DescribeAppInstanceUser	Accorde l'autorisation d'obtenir tous les détails d'un AppInstanceUser	Lecture	app-instance-user*		
DescribeAppInstanceUserEndpoint	Accorde l'autorisation de décrire un point de terminaison enregistré pour un utilisateur d'instance d'application	Lecture	app-instance-user*		
DescribeChannel	Accorde l'autorisation d'obtenir toutes les informations d'une chaîne.	Lecture	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelBan	Accorde l'autorisation d'obtenir toutes les informations relatives à l'exclusion d'une chaîne.	Lecture	app-instance-bot*		
			app-instance-user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			channel*		
DescribeChannelFlow	Accorde l'autorisation d'obtenir toutes les informations d'un flux de canal	Lecture	channel-flow*		
DescribeChannelMembership	Accorde l'autorisation d'obtenir toutes les informations relatives à l'abonnement à une chaîne.	Lecture	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelMembershipForAppInstanceUser	Octroie l'autorisation d'obtenir des informations d'un canal en fonction de l'appartenance de l'utilisateur ou du bot spécifié	Lecture	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModeratedByAppInstanceUser	Octroie l'autorisation d'obtenir toutes les informations relatives à un canal modéré par l'utilisateur ou le bot spécifié	Lecture	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModerator	Donne l'autorisation d'obtenir tous les détails d'un single ChannelModerator	Lecture	app-instance-bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			app-instance-user*		
			channel*		
DisassociateChannelFlow	Accorde l'autorisation de dissocier un flux d'un canal	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		
DisassociatePhoneNumberFromUser	Accorde l'autorisation de dissocier le numéro principal fourni de l'utilisateur Amazon Chime spécifié.	Écriture			
DisassociatePhoneNumbersFromVoiceConnector	Accorde l'autorisation de dissocier plusieurs numéros de téléphone du Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
DisassociatePhoneNumbersFromVoiceConnectorGroup	Accorde l'autorisation de dissocier plusieurs numéros de téléphone du groupe de Amazon Chime Voice Connector spécifié	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateSigninDelegateGroupsFromAccount	Accorde l'autorisation de dissocier les groupes de délégués de connexion spécifiés du compte Amazon Chime spécifié	Écrire			
DisassociateVoiceConnectorConnect [autorisation uniquement]	Accorde l'autorisation de dissocier l'instance Amazon Connect du connecteur vocal Amazon Chime spécifié	Écrire			
DisconnectDirectory	Accorde l'autorisation de déconnecter un répertoire Active Directory de votre compte Amazon Chime de type entreprise	Écriture			
GetAccount	Accorde l'autorisation d'obtenir des détails pour le compte Amazon Chime spécifié	Lecture			
GetAccountResource	Accorde l'autorisation d'obtenir des détails pour la ressource du compte associée à votre compte Amazon Chime	Lecture			
GetAccountSettings	Accorde l'autorisation d'obtenir des paramètres de compte pour l'ID de compte Amazon Chime spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountWithOpenIdConfig	Accorde l'autorisation d'obtenir les détails et OpenIdConfig les attributs de votre compte Amazon Chime	Lecture			
GetAppInstanceRetentionSettings	Accorde l'autorisation d'obtenir des paramètres de rétention pour une instance d'application.	Lecture	app-instance*		
GetAppInstanceStreamingConfigurations	Accorde l'autorisation d'obtenir des configurations de streaming pour une instance d'application.	Lecture	app-instance*		
GetAttendee	Accorde l'autorisation d'obtenir les détails du participant pour un ID de réunion et un ID de participant spécifiés	Lecture	meeting*		
GetBot	Accorde l'autorisation de récupérer des détails pour le bot spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCDRBucket	Accorde l'autorisation d'obtenir les détails d'un compartiment Call Detail Record S3 associé à votre compte Amazon Chime	Lecture			s3:GetBucketAcl s3:GetBucketLocation s3:GetBucketLogging s3:GetBucketVersioning s3:GetBucketWebsite
GetChannelMembershipPreferences	Accorde l'autorisation d'obtenir les préférences relatives à l'abonnement à une chaîne	Lecture	app-instance-bot*		
			app-instance-user*		
			channel*		
GetChannelMessage	Accorde l'autorisation d'obtenir toutes les informations d'un message de chaîne.	Lecture	app-instance-bot*		
			app-instance-user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			channel*		
GetChannelMessageStatus	Accorde l'autorisation d'obtenir toutes les informations d'un message de canal	Lecture	app-instance-bot*		
			app-instance-user*		
			channel*		
GetDomain	Accorde l'autorisation d'obtenir les détails de domaine pour un domaine associé à votre compte Amazon Chime	Lecture			
GetEventsConfiguration	Accorde l'autorisation de récupérer les détails d'une configuration d'événements pour qu'un bot puisse recevoir des événements sortants.	Lecture			
GetGlobalSettings	Octroie l'autorisation d'obtenir les paramètres globaux relatifs à Amazon Chime pour Compte AWS	Lecture			
GetMediaCapturePipeline	Accorde l'autorisation d'obtenir un pipeline de capture du média existant	Lecture	media-pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMediaInsightsPipelineConfiguration	Octroie l'autorisation d'obtenir une configuration de pipeline d'informations multimédias	Lecture	media-insights-pipeline-configuration*		
GetMediaPipeline	Accorde l'autorisation d'obtenir un pipeline du média existant	Lecture	media-pipeline*		
GetMediaPipelineKinesisVideoStreamPool	Accorde l'autorisation d'obtenir un pipeline du média existant	Lecture	media-pipeline-kinesis-video-stream-pool*		
GetMeeting	Accorde l'autorisation d'obtenir l'enregistrement de la réunion pour un ID de réunion spécifié	Lecture	meeting*		
GetMeetingDetail	Accorde l'autorisation d'obtenir des détails de participant, de connexion, et d'autres détails pour une réunion	Lecture			
GetMessagingSessionEndpoint	Accorde l'autorisation d'obtenir le point de terminaison pour la session de messagerie.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMessagingStreamingConfigurations	Accorde l'autorisation d'obtenir les configurations de streaming de données d'un AppInstance	Lecture	app-instance*		
GetPhoneNumber	Accorde l'autorisation d'obtenir des détails pour le numéro de téléphone spécifié	Lecture			
GetPhoneNumberOrder	Accorde l'autorisation d'obtenir des détails pour la commande de numéro de téléphone spécifié	Lecture			
GetPhoneNumberSettings	Octroie l'autorisation d'obtenir les paramètres du numéro de téléphone relatifs à Amazon Chime pour Compte AWS	Lecture			
GetProxySession	Accorde l'autorisation d'obtenir les détails de la session proxy spécifiée pour le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		
GetRetentionSettings	Accorde l'autorisation de récupérer les paramètres de conservation pour le compte Amazon Chime spécifié	Lecture			
GetRoom	Accorde l'autorisation de récupérer une salle	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSipMediaApplication	Accorde l'autorisation d'obtenir des informations sur l'application multimédia Amazon Chime SIP auprès de l'administrateur Compte AWS	Lecture	sip-media-application*		
GetSipMediaApplicationAlexaSkillConfiguration	Octroie l'autorisation d'obtenir les paramètres de configuration Alexa Skill pour l'application multimédia Amazon Chime SIP sous le Compte AWS	Lecture	sip-media-application*		
GetSipMediaApplicationLoggingConfiguration	Accorde l'autorisation d'obtenir les paramètres de configuration de journalisation pour l'application multimédia Amazon Chime SIP auprès de l'administrateur Compte AWS	Lecture	sip-media-application*		
GetSipRule	Accorde l'autorisation d'obtenir les détails de la règle SIP d'Amazon Chime auprès de l'administrateur Compte AWS	Lecture			
GetSpeakerSearchTask	Accorde l'autorisation d'obtenir une tâche de recherche de haut-parleur sur la ressource Amazon Chime spécifiée.	Lecture	media-pipeline voice-connector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTelephonyLimits	Accorde l'autorisation d'obtenir des limites de téléphonie pour Compte AWS	Lecture			
GetUser	Accorde l'autorisation d'obtenir des détails pour l'ID d'utilisateur spécifié	Lecture			
GetUserActivityReportData	Accorde l'autorisation d'obtenir un récapitulatif de l'activité de l'utilisateur sur la page des détails de l'utilisateur	Lecture			
GetUserByEmail	Accorde l'autorisation de récupérer les informations d'un utilisateur Amazon Chime en fonction de l'adresse e-mail dans un compte Amazon Chime de type équipe ou entreprise	Lecture			
GetUserSettings	Accorde l'autorisation d'obtenir les paramètres utilisateur liés à l'utilisateur Amazon Chime spécifié	Lecture			
GetVoiceConnector	Accorde l'autorisation d'obtenir des détails sur le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetVoiceConnectorEmergencyCallingConfiguration	Accorde l'autorisation d'obtenir les détails de la configuration des appels d'urgence pour le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		
GetVoiceConnectorExternalSystemsConfiguration	Accorde l'autorisation d'obtenir la configuration du système externe connecté au connecteur vocal Amazon Chime spécifié	Lecture	voice-connector*		
GetVoiceConnectorGroup	Accorde l'autorisation d'obtenir des détails sur le groupe de Amazon Chime Voice Connector spécifié	Lecture			
GetVoiceConnectorLoggingConfiguration	Accorde l'autorisation d'obtenir les détails de la configuration de journalisation pour le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		
GetVoiceConnectorOrigination	Accorde l'autorisation d'obtenir les détails des paramètres de création pour le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetVoiceConnectorProxy	Accorde l'autorisation d'obtenir les détails de la configuration de proxy pour le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		
GetVoiceConnectorStreamingConfiguration	Accorde l'autorisation d'obtenir les détails de la configuration du streaming pour le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		
GetVoiceConnectorTermination	Accorde l'autorisation d'obtenir les détails des paramètres de résiliation pour le Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		
GetVoiceConnectorTerminationHealth	Permet d'obtenir les détails de l'état de la résiliation du Amazon Chime Voice Connector spécifié	Lecture	voice-connector*		
GetVoiceProfile	Octroie l'autorisation d'obtenir un profil vocal	Lecture	voice-profile*		
GetVoiceProfileDomain	Octroie l'autorisation d'obtenir un domaine de profil vocal	Lecture	voice-profile-domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetVoiceToneAnalysisTask	Accorde l'autorisation d'obtenir une tâche d'analyse de tonalités vocales sur la ressource Amazon Chime spécifiée.	Lecture	media-pipeline		
			voice-connector		
InviteDelegate	Accorde l'autorisation d'envoyer une invitation pour accepter une demande de Compte AWS délégation pour un compte Amazon Chime	Écrire			
InviteUsers	Accorde l'autorisation d'inviter 50 utilisateurs maximum sur compte Amazon Chime spécifié	Écriture			
InviteUsersFromProvider	Accorde l'autorisation d'inviter des utilisateurs d'un fournisseur tiers dans votre compte Amazon Chime	Écriture			
ListAccountUsageReportData	Accorde l'autorisation de répertorier les données de rapport d'utilisation du compte Amazon Chime	List			
ListAccounts	Accorde l'autorisation de répertorier les comptes Amazon Chime sous le nom de l'administrateur Compte AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApiKeys	Accorde l'autorisation de répertorier les clés d'accès SCIM définies pour votre compte Amazon Chime et votre configuration Okta	Liste			
ListAppInstanceAdmins	Accorde l'autorisation de répertorier les administrateurs dans l'instance d'application.	List	app-instance*		
			app-instance-bot*		
			app-instance-user*		
ListAppInstanceBots	Accorde l'autorisation de répertorier toutes les AppInstanceBots données créées sous une seule instance d'application	List	app-instance-bot*		
ListAppInstanceUserEndpoints	Accorde l'autorisation de répertorier les points de terminaison enregistrés pour un utilisateur d'instance d'application	List	app-instance-user*		
ListAppInstanceUsers	Accorde l'autorisation de répertorier toutes les AppInstanceUsers données créées sous une seule instance d'application	List	app-instance-user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAppInstances	Accorde l'autorisation de répertorier toutes les instances d'application Amazon Chime créées sous une seule Compte AWS	List	app-instance*		
ListAttendeeTags	Accorde l'autorisation de répertorier les balises appliquées à une ressource de participant du kit SDK d'Amazon Chime	Liste	meeting*		
ListAttendees	Accorde l'autorisation de répertorier jusqu'à 100 participants pour une réunion du SDK d'Amazon Chime spécifiée	List	meeting*		
ListAvailableVoiceConnectorRegions	Autorise à répertorier les fichiers disponibles Régions AWS dans lesquels vous pouvez créer un connecteur vocal Amazon Chime SDK	List			
ListBots	Accorde l'autorisation de répertorier les bots associés au compte Amazon Chime de type entreprise de l'administrateur	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCDRBucket	Accorde l'autorisation de répertorier des compartiments Call Detail Record S3	List			s3:ListAllMyBuckets s3:ListBucket
ListCallingRegions	Accorde l'autorisation de répertorier les régions d'appel disponibles pour l'administrateur Compte AWS	List			
ListChannelBans	Octroie l'autorisation de répertorier tous les utilisateurs et bots exclus d'un canal particulier	List	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelFlows	Permet de répertorier tous les flux de canaux créés sous un seul carillon AppInstance	List	channel-flow*		
ListChannelMemberships	Accorde l'autorisation de répertorier tous les abonnés à une chaîne.	List	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListChannelMembershipsForAppInstanceUser	Octroie l'autorisation de répertorier tous les canaux dont un utilisateur ou un bot particulier fait partie	List	app-instance-bot*		
			app-instance-user*		
ListChannelMessages	Accorde l'autorisation de répertorier tous les messages d'une chaîne	Lecture	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelModerators	Accorde l'autorisation de répertorier tous les modérateurs pour une chaîne	List	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannels	Permet de répertorier toutes les chaînes créées sous un seul carillon AppInstance	List	app-instance-bot*		
			app-instance-user*		
ListChannelsAssociatedWithChannelFlow	Accorde l'autorisation de répertorier tous les canaux associés à un seul flux de canal Chime	List	channel-flow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListChannelsModeratedByAppInstanceUser	Octroie l'autorisation de répertorier tous les canaux modérés par un utilisateur ou un bot	List	app-instance-bot* app-instance-user*		
ListDelegates	Accorde l'autorisation de répertorier les informations de délégué de compte associées à votre compte Amazon Chime	List			
ListDirectories	Permet de répertorier les Active Directory actifs hébergés dans le Directory Service de votre Compte AWS	List			
ListDomains	Accorde l'autorisation de répertorier les domaines associés à votre compte Amazon Chime	Liste			
ListGroups	Accorde l'autorisation de répertorier les groupes d'utilisateurs Active Directory ou Okta associés à votre compte Amazon Chime de type entreprise	Liste			
ListMediaCapturePipelines	Accorde l'autorisation de répertorier les pipelines de capture du média	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMediaInsightsPipelineConfigurations	Octroie l'autorisation de répertorier toutes les configurations de pipeline d'informations multimédias	List			
ListMediaPipelineKinesisVideoStreamPools	Accorde l'autorisation de répertorier les pipelines du média	List			
ListMediaPipelines	Accorde l'autorisation de répertorier les pipelines du média	List			
ListMeetingEvents	Accorde l'autorisation de répertorier tous les événements qui se sont produits pendant une réunion particulière	List			
ListMeetingTags	Accorde l'autorisation de répertorier les balises appliquées à une ressource de réunion du kit SDK d'Amazon Chime	List	meeting*		
ListMeetings	Accorde l'autorisation de répertorier jusqu'à 100 réunions actives du kit SDK d'Amazon Chime	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMeetingsReportData	Accorde l'autorisation de répertorier les réunions terminées au cours de la plage de dates spécifiée	List			
ListPhoneNumberOrders	Accorde l'autorisation de répertorier les commandes par numéro de téléphone sous le nom de l'administrateur Compte AWS	List			
ListPhoneNumbers	Accorde l'autorisation de répertorier les numéros de téléphone sous le nom de l'administrateur Compte AWS	List			
ListProxySessions	Accorde l'autorisation de répertorier les sessions de proxy pour le Amazon Chime Voice Connector spécifié	Liste	voice-connector*		
ListRoomMemberships	Accorde l'autorisation de répertorier tous les membres de la salle	Liste			
ListRooms	Accorde l'autorisation de répertorier les salles	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSipMediaApplications	Permet de répertorier toutes les applications multimédia Amazon Chime SIP sous le nom de l'administrateur Compte AWS	List			
ListSipRules	Autorise l'administrateur à répertorier toutes les règles SIP d'Amazon Chime Compte AWS	List	sip-media-application		
ListSubChannels	Permet de tout répertorier SubChannels sous une seule chaîne	List	app-instance-bot*		
			app-instance-user*		
			channel*		
ListSupportedPhoneNumberCountries	Accorde l'autorisation de répertorier les numéros de téléphone des pays pris en charge par le Compte AWS	List			
ListTagsForResource	Accorde l'autorisation de répertorier des balises appliquées à une ressource Amazon Chime	Lecture	app-instance		
			app-instance-bot		
			app-instance-user		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			channel		
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			voice-profile-domain		
ListUsers	Accorde l'autorisation de répertorier les utilisateurs qui appartiennent au compte Amazon Chime spécifié	List			
ListVoiceConnectorGroups	Accorde l'autorisation de répertorier les groupes Amazon Chime Voice Connector sous le nom de l'administrateur Compte AWS	List			
ListVoiceConnectorTerminationCredentials	Accorde l'autorisation de répertorier les informations d'identification de résiliation SIP pour le Amazon Chime Voice Connector spécifié	List	voice-connector*		
ListVoiceConnectors	Accorde l'autorisation de répertorier les connecteurs vocaux Amazon Chime sous le nom de l'administrateur Compte AWS	List			
ListVoiceProfileDomains	Octroie l'autorisation de répertorier les domaines de profil vocal	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListVoiceProfiles	Octroie l'autorisation de répertorier les profils vocaux	List	voice-profile-domain*		
LogoutUser	Accorde l'autorisation de déconnecter l'utilisateur spécifié à partir de tous les appareils qui sont actuellement connectés	Écriture			
PutAppInstanceRetentionSettings	Accorde l'autorisation d'activer la rétention des données pour l'instance d'application.	Écriture	app-instance*		
PutAppInstanceStreamingConfigurations	Accorde l'autorisation de configurer le streaming de données pour l'instance d'application.	Écrire	app-instance*		
PutAppInstanceUserExpirationSettings	Accorde l'autorisation de définir les paramètres d'expiration d'un AppInstanceUser	Écrire	app-instance-user*		
PutChannelExpirationSettings	Octroie l'autorisation de définir des paramètres d'expiration pour un canal	Écrire	app-instance-user* channel*		
PutChannelMembershipPreferences	Accorde l'autorisation de définir les préférences relatives à l'abonnement à une chaîne	Écrire	app-instance-bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			app-instance-user*		
			channel*		
PutEventsConfiguration	Accorde l'autorisation de mettre à jour les détails de configuration d'événements pour qu'un bot puisse recevoir les événements sortants	Écrire			
PutMessagingStreamingConfigurations	Accorde l'autorisation de mettre en place les configurations de streaming de données d'un AppInstance	Écrire	app-instance*		
PutRetentionSettings	Accorde l'autorisation de créer ou mettre à jour les paramètres de conservation pour le compte Amazon Chime spécifié	Écrire			
PutSipMediaApplicationAlexaSkillConfiguration	Autorise la mise à jour des paramètres de configuration Alexa Skill pour l'application multimédia Amazon Chime SIP sous le nom de l'administrateur Compte AWS	Écrire	sip-media-application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutSipMediaApplicationLoggingConfiguration	Accorde l'autorisation de mettre à jour les paramètres de configuration de journalisation pour l'application multimédia Amazon Chime SIP sous le Compte AWS	Écrire	sip-media-application*		
PutVoiceConnectorEmergencyCallingConfiguration	Accorde l'autorisation d'ajouter la configuration des appels d'urgence pour le Amazon Chime Voice Connector spécifié	Écrire	voice-connector*		
PutVoiceConnectorExternalSystemsConfiguration	Accorde l'autorisation de mettre à jour la configuration du système externe connecté au connecteur vocal Amazon Chime spécifié	Écrire	voice-connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutVoiceConnectorLoggingConfiguration	Accorde l'autorisation d'ajouter la configuration de journalisation pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:GetLogDelivery logs:ListLogDeliveries
PutVoiceConnectorOrigination	Accorde l'autorisation de mettre à jour les paramètres de création pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutVoiceConnectorProxy	Accorde l'autorisation d'ajouter la configuration de proxy pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
PutVoiceConnectorStreamingConfiguration	Accorde l'autorisation d'ajouter une configuration de streaming pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		chime:GetMediaInsightsPipelineConfiguration
			media-insights-pipeline-configuration		
PutVoiceConnectorTermination	Accorde l'autorisation de mettre à jour les paramètres de résiliation pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
PutVoiceConnectorTerminationCredentials	Accorde l'autorisation d'ajouter les informations d'identification de résiliation SIP pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
RedactChannelMessage	Accorde l'autorisation de rédiger le contenu du message.	Écrire	app-instance-bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			app-instance-user*		
			channel*		
RedactConversationMessage	Accorde l'autorisation de rédiger le message de conversation Chime spécifié	Écrire			
RedactRoomMessage	Accorde l'autorisation de rédiger le message de salle Chime spécifié	Écrire			
RegenerateSecurityToken	Accorde l'autorisation de régénérer le jeton de sécurité pour le bot spécifié	Écrire			
RegisterAppInstanceUserEndpoint	Accorde l'autorisation d'enregistrer un point de terminaison pour un utilisateur d'instance d'application	Écrire	app-instance-user*		mobiletargeting:GetApp
RenameAccount	Accorde l'autorisation de modifier le nom du compte pour les comptes Amazon Chime de type entreprise ou équipe	Écriture			
RenewDelegate	Accorde l'autorisation de renouveler la demande de délégations associée à un compte Amazon Chime	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResetAccountResource	Accorde l'autorisation de réinitialiser la ressource de compte dans votre compte Amazon Chime	Écriture			
ResetPersonalPIN	Accorde l'autorisation de réinitialiser le code PIN de réunion personnelle pour l'utilisateur spécifié dans un compte Amazon Chime	Écriture			
RestorePhoneNumber	Accorde l'autorisation de restaurer le numéro de téléphone spécifié à partir de la file d'attente de suppression dans le numéro de téléphone de l'inventaire	Écriture			
RetrieveDataExports	Accorde l'autorisation de télécharger le fichier contenant des liens vers toutes les pièces jointes renvoyées dans le cadre de l'action « Request attachments » (Demande de pièces jointes)	Lecture			
SearchAvailablePhoneNumbers	Accorde l'autorisation de rechercher des numéros de téléphone pouvant être commandés auprès de l'opérateur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchChannels	Accorde l'autorisation de rechercher des chaînes auxquelles AppInstanceUser appartient un ou de AppInstance rechercher des chaînes sur un AppInstaceAdmin	List	app-instance-bot*		
			app-instance-user*		
SendChannelMessage	Accorde l'autorisation d'envoyer un message à une chaîne particulière indiquant que le membre fait partie de	Écriture	app-instance-bot*		
			app-instance-user*		
			channel*		
StartDataExport	Accorde l'autorisation de soumettre la demande « Request attachments » (Demande de pièces jointes)	Écrire			
StartMeetingTranscription	Accorde l'autorisation de démarrer la transcription pour une réunion	Écrire			
StartSpeakerSearchTask	Accorde l'autorisation de démarrer une tâche de recherche de haut-parleur sur la ressource Amazon Chime spécifiée.	Écrire	media-pipeline		
			voice-connector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartVoiceToneAnalysisTask	Accorde l'autorisation de démarrer une tâche d'analyse de tonalités vocales sur la ressource Amazon Chime spécifiée.	Écrire	media-pipeline		
			voice-connector		
StopMeetingTranscription	Accorde l'autorisation d'arrêter la transcription pour une réunion	Écrire			
StopSpeakerSearchTask	Accorde l'autorisation d'arrêter une tâche de recherche de haut-parleur sur la ressource Amazon Chime spécifiée.	Écrire	media-pipeline		
			voice-connector		
StopVoiceToneAnalysisTask	Accorde l'autorisation d'arrêter une tâche d'analyse de tonalités vocales sur la ressource Amazon Chime spécifiée.	Écrire	media-pipeline		
			voice-connector		
SubmitSupportRequest	Accorde l'autorisation de soumettre une demande de prise en charge du service client	Écriture			
SuspendUsers	Accorde l'autorisation de suspendre des utilisateurs d'un compte Amazon Chime de type entreprise	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagAttendee	Accorde l'autorisation d'appliquer les balises spécifiées au participant du kit SDK d'Amazon Chime spécifié	Identification	meeting*		
TagMeeting	Accorde l'autorisation d'appliquer les balises spécifiées à la réunion du kit SDK d'Amazon Chime spécifiée	Identification	meeting*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation d'appliquer les balises spécifiées à la ressource spécifiée (les contrôles d'accès basés sur des balises ne sont pris en charge que sur *-chime). (points de <region>terminaison .amazonaws.com)	Identification	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnauthorizeDirectory	Accorde l'autorisation de désapprouver un répertoire Active Directory de votre compte Amazon Chime de type entreprise	Écrire			
UntagAttendee	Accorde l'autorisation de retirer les balises spécifiées du participant du kit SDK d'Amazon Chime spécifié	Identification	meeting*		
UntagMeeting	Accorde l'autorisation de retirer les balises spécifiées de la réunion du kit SDK d'Amazon Chime spécifiée	Identification	meeting*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de dissocier les balises spécifiées de la ressource spécifiée (les contrôles d'accès basés sur des balises ne sont pris en charge que sur *-chime). (points de <region>terminaison .amazonaws.com)	Identification	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			sip-media-application		
			voice-connector		
			voice-profile-domain		
				aws:TagKeys	
UpdateAccount	Accorde l'autorisation de mettre à jour les détails du compte pour le compte Amazon Chime spécifié	Écrire			
UpdateAccountOpenIdConfig	Autorise la mise à jour des OpenIdConfig attributs de votre compte Amazon Chime	Écrire			
UpdateAccountResource	Accorde l'autorisation de mettre à jour la ressource de compte dans votre compte Amazon Chime	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAccountSettings	Accorde l'autorisation de mettre à jour les paramètres pour le compte Amazon Chime spécifié	Écrire			
UpdateAppInstance	Accorde l'autorisation de mettre à jour AppInstance les métadonnées	Écrire	app-instance*		
UpdateAppInstanceBot	Accorde l'autorisation de mettre à jour les informations d'un AppInstanceBot	Écrire	app-instance-bot*		
UpdateAppInstanceUser	Accorde l'autorisation de mettre à jour les informations d'un AppInstanceUser	Écrire	app-instance-user*		
UpdateAppInstanceUserEndpoint	Accorde l'autorisation de mettre à jour un point de terminaison enregistré pour un utilisateur d'instance d'application	Écrire	app-instance-user*		
UpdateAttendeeCapabilities	Accorder l'autorisation aux capacités que vous souhaitez mettre à jour	Écrire	meeting*		
UpdateBot	Accorde l'autorisation de mettre à jour le statut du bot spécifié	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCDRSettings	Accorde l'autorisation de mettre à jour votre compartiment Call Detail Record S3	Écriture			s3:CreateBucket s3:DeleteBucket s3:ListAllMyBuckets
UpdateChannel	Accorde l'autorisation de mettre à jour des attributs d'une chaîne.	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelFlow	Accorde l'autorisation de mettre à jour un flux de chaîne	Écrire	channel-flow*		
UpdateChannelMessage	Accorde l'autorisation de mettre à jour le contenu d'un message.	Écriture	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateChannelReadMarker	Accorde l'autorisation de définir l'horodatage au moment où un utilisateur a lu pour la dernière fois les messages dans une chaîne.	Écrire	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateGlobalSettings	Autorise la mise à jour des paramètres globaux relatifs à Amazon Chime pour Compte AWS	Écrire			
UpdateMediaInsightsPipelineConfiguration	Octroie l'autorisation de mettre à jour le statut d'une configuration de pipeline d'informations multimédias	Écrire	media-insights-pipeline-configuration*		chime:ListVoiceConnectors iam:PassRole kinesis:DescribeStream s3:ListBucket
UpdateMediaInsightsPipelineStatus	Octroie l'autorisation de mettre à jour le statut d'un pipeline d'informations multimédias	Écrire	media-pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMediaPipelineKinesisVideoStreamPool	Accorde l'autorisation de mettre à jour un groupe de flux vidéo Kinesis.	Écrire	media-pipeline-kinesis-video-stream-pool*		
UpdatePhoneNumber	Accorde l'autorisation de mettre à jour des détails de numéro de téléphone pour le numéro de téléphone spécifié	Écrire			
UpdatePhoneNumberSettings	Accorde l'autorisation de mettre à jour les paramètres du numéro de téléphone relatifs à Amazon Chime pour le Compte AWS	Écrire			
UpdateProxySession	Accorde l'autorisation de mettre à jour une session de proxy pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
UpdateRoom	Accorde l'autorisation de mettre à jour une salle	Écriture			
UpdateRoomMembership	Accorde l'autorisation de mettre à jour le rôle d'appartenance à la salle	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSipMediaApplication	Autorise la mise à jour des propriétés de l'application multimédia Amazon Chime SIP sous le nom de l'administrateur Compte AWS	Écrire	sip-media-application*		
UpdateSipMediaApplicationCall	Octroie l'autorisation de mettre à jour un appel d'application multimédia Amazon Chime SIP sous le Compte AWS	Écrire	sip-media-application*		
UpdateSipRule	Autorise l'administrateur à mettre à jour les propriétés de la règle SIP Amazon Chime Compte AWS	Écrire	sip-media-application		
UpdateSupportedLicenses	Accorde l'autorisation de mettre à jour la prise en charge des niveaux de licence disponibles pour les utilisateurs de votre compte Amazon Chime	Écriture			
UpdateUser	Accorde l'autorisation de mettre à jour les détails utilisateur pour un ID d'utilisateur spécifié	Écriture			
UpdateUserLicenses	Accorde l'autorisation de mettre à jour les licences pour vos utilisateurs Amazon Chime	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateUserSettings	Accorde l'autorisation de mettre à jour les paramètres utilisateur liés à l'utilisateur Amazon Chime spécifié	Écriture			
UpdateVoiceConnector	Accorde l'autorisation de mettre à jour les détails du Amazon Chime Voice Connector pour le Amazon Chime Voice Connector spécifié	Écriture	voice-connector*		
UpdateVoiceConnectorGroup	Accorde l'autorisation de mettre à jour les détails du groupe de Amazon Chime Voice Connector pour le groupe de Amazon Chime Voice Connector spécifié	Écrire	voice-connector		
UpdateVoiceProfile	Octroie l'autorisation de mettre à jour un profil vocal	Écrire	voice-profile*		
UpdateVoiceProfileDomain	Octroie l'autorisation de mettre à jour un domaine de profil vocal	Écrire	voice-profile-domain*		
ValidateAccountResource	Accorde l'autorisation de valider la ressource de compte dans votre compte Amazon Chime	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ValidateE911Address	Accorde l'autorisation de valider une adresse à utiliser pour les appels au 911 effectués avec les connecteurs vocaux Amazon Chime	Lecture			

Types de ressources définis par Amazon Chime

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
meeting	`arn:${Partition}:chime:${Region}:${AccountId}:meeting/${MeetingId}`	aws:ResourceTag/${TagKey}
app-instance	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}`	aws:ResourceTag/${TagKey}
app-instance-user	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/user/${AppInstanceUserId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
app-instance-bot	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/bot/${AppInstanceBotId}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel/${ChannelId}	aws:ResourceTag/${TagKey}
channel-flow	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel-flow/${ChannelFlowId}	aws:ResourceTag/${TagKey}
media-pipeline	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline/${MediaPipelineId}	aws:ResourceTag/${TagKey}
media-insights-pipeline-configuration	arn:${Partition}:chime:${Region}:${AccountId}:media-insights-pipeline-configuration/${ConfigurationName}	aws:ResourceTag/${TagKey}
media-pipeline-kinesis-video-stream-pool	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline-kinesis-video-stream-pool/${PoolName}	aws:ResourceTag/${TagKey}
voice-profile-domain	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile-domain/${VoiceProfileDomainId}	aws:ResourceTag/${TagKey}
voice-profile	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile/${VoiceProfileId}	

Types de ressources	ARN	Clés de condition
voice-connector	`arn:${Partition}:chime:${Region}:${AccountId}:vc/${VoiceConnectorId}`	aws:ResourceTag/${TagKey}
sip-media-application	`arn:${Partition}:chime:${Region}:${AccountId}:sma/${SipMediaApplicationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Chime

Amazon Chime définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString

Actions, ressources et clés de condition pour Claude Platform sur AWS

Claude Platform on AWS (préfixe de service :`aws-external-anthropic`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Claude Platform sur AWS
- Types de ressources définis par Claude Platform sur AWS
- Clés de condition pour Claude Platform on AWS

Actions définies par Claude Platform sur AWS

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ArchiveWorkspace	Accorde l'autorisation d'archiver un espace de travail	Écrire	workspace *		
AssumeConsole	Accorde l'autorisation d'accéder à la console sur la plateforme Claude	Écrire		aws-external-anthropic:Capability	
CallWithBearerToken	Accorde l'autorisation d'effectuer des appels d'API à l'aide	List		aws-external-anthropic:Bear	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]	de l'authentification par jeton porteur			erTokenType	
CancelBatchInference	Autorise l'annulation d'une demande d'inférence par lots en cours	Écrire	workspace*		
CountTokens	Accorde l'autorisation de compter les jetons pour une demande de message	Écrire	workspace*		
CreateBatchInference	Accorde l'autorisation de créer une demande d'inférence par lots	Écrire	workspace*		
CreateFile	Accorde l'autorisation de télécharger un fichier dans un espace de travail	Écrire	workspace*		
CreateInference	Accorde l'autorisation de créer une demande d'inférence de fin de chat	Écrire	workspace*		
CreateSkill	Accorde l'autorisation de créer une compétence dans un espace de travail	Écrire	workspace*		
CreateUserProfile	Accorde l'autorisation de créer un profil utilisateur dans un espace de travail	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkspace	Accorde l'autorisation de créer un espace de travail dans une organisation	Écrire			
DeleteBatchInference	Accorde l'autorisation de supprimer une demande d'inférence par lots	Écrire	workspace*		
DeleteFile	Accorde l'autorisation de supprimer un fichier d'un espace de travail	Écrire	workspace*		
DeleteSkill	Accorde l'autorisation de supprimer une compétence d'un espace de travail	Écrire	workspace*		
GetAccountStatus	Accorde l'autorisation de récupérer l'état de la configuration et de l' AWS Marketplace enregistrement du compte	Lecture			
GetBatchInference	Accorde l'autorisation de récupérer les détails d'une demande d'inférence par lots	Lecture	workspace*		
GetFile	Accorde l'autorisation de récupérer un fichier ou son contenu depuis un espace de travail	Lecture	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetModel	Accorde l'autorisation de récupérer des informations sur un modèle spécifique	Lecture	workspace*		
GetSkill	Accorde l'autorisation de récupérer les détails d'une compétence ou de ses versions	Lecture	workspace*		
GetUserProfile	Accorde l'autorisation de récupérer les détails d'un profil utilisateur	Lecture	workspace*		
GetWorkspace	Accorde l'autorisation de récupérer les détails d'un espace de travail	Lecture	workspace*		
ListBatchInferences	Accorde l'autorisation de répertorier les demandes d'inférence par lots dans un espace de travail	List	workspace*		
ListFiles	Accorde l'autorisation de répertorier des fichiers dans un espace de travail	List	workspace*		
ListModels	Accorde l'autorisation de répertorier les modèles disponibles dans un espace de travail	List	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSkills	Accorde l'autorisation de répertorier les compétences dans un espace de travail	List	workspace*		
ListUserProfiles	Accorde l'autorisation de répertorier les profils utilisateur dans un espace de travail	List	workspace*		
ListWorkspaces	Accorde l'autorisation de répertorier les espaces de travail d'une organisation	List			
UpdateSkill	Accorde l'autorisation de créer ou de supprimer une version de compétence	Écrire	workspace*		
UpdateUserProfile	Accorde l'autorisation de mettre à jour un profil utilisateur dans un espace de travail	Écrire	workspace*		
UpdateWorkspace	Accorde l'autorisation de mettre à jour un espace de travail	Écrire	workspace*		

Types de ressources définis par Claude Platform sur AWS

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workspace	`arn:${Partition}:aws-external-anthropic:${Region}:${Account}:workspace/${ResourceId}`	

Clés de condition pour Claude Platform on AWS

Claude Platform on AWS définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws-external-anthropic:BearerTokenType	Filtre l'accès par les jetons porteurs à court ou à long terme	String
aws-external-anthropic:Capability	Filtre l'accès en fonction du rôle Claude Platform utilisé pour la session de console	String

Actions, ressources et clés de condition pour les salles AWS blanches

AWS Clean Rooms (préfixe de service :`cleanrooms`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Clean Rooms
- Types de ressources définis par AWS Clean Rooms
- Clés d'état pour les salles AWS propres

Actions définies par AWS Clean Rooms

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetCollaborationAnalysisTemplate	Octroie l'autorisation d'afficher les détails des modèles analysisTemplates associés à la collaboration.	Lecture	analysistemplate*		cleanrooms:GetCollaborationAnalysisTemplate
			collaboration*		
BatchGetSchema	Accorde l'autorisation d'afficher les détails des schémas	Lecture	collaboration*		cleanrooms:GetSchema

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			configuredtableassociation		
			idmappingtable		
BatchGetSchemaAnalysisRule	Autorise l'affichage des règles d'analyse associées aux schémas	Lecture	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		
CreateAnalysisTemplate	Octroie l'autorisation de créer un nouveau modèle d'analyse.	Écrire	analysistemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollaboration	Accorde l'autorisation de créer une nouvelle collaboration, un environnement de collaboration de données partagées	Écrire	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollaborationChangeRequest	Accorde l'autorisation de créer une demande de modification dans une collaboration	Écrire	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfiguredAudienceModelAssociation	Octroie l'autorisation de lier un modèle d'audience configuré par Cleanrooms ML à une collaboration en créant une nouvelle association.	Écrire	configuredaudiencemodelassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	cleanrooms-ml:GetConfiguredAudienceModel cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfiguredTable	Accorde l'autorisation de créer un nouveau tableau configuré	Écrire	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	athena:GetTableMetadata glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions glue:GetSchemaVersion glue:GetTable glue:GetTables

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfiguredTableAnalysisRule	Accorde l'autorisation de créer une règle d'analyse pour un tableau configuré	Écrire	configuredtable*		
CreateConfiguredTableAssociation	Accorde l'autorisation de lier un tableau configuré à une collaboration en créant une nouvelle association	Écrire	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole
			configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateConfiguredTableAssociationAnalysisRule	Accorde l'autorisation de créer une règle d'analyse pour une association de tables configurée	Écrire	configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdMappingTable	Accorde l'autorisation de lier un flux de travail de mappage d'identifiants à une collaboration en créant une nouvelle table de mappage d'identifiants	Écrire	idmappingtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdMappingWorkflow

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdNamespaceAssociation	Accorde l'autorisation de lier un espace de noms d'identifiant de résolution d' AWS entité à une collaboration en créant une nouvelle association	Écrire	idnamespaceassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdNamespace
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMembership	Accorde l'autorisation de rejoindre des collaborations en créant une adhésion	Écrire	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivacyBudgetTemplate	Octroie l'autorisation de créer un modèle budgétaire de confidentialité.	Écrire	membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			privacybudgettemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteAnalysisTemplate	Octroie l'autorisation de supprimer un modèle d'analyse existant.	Écrire	analysistemplate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCollaboration	Accorde l'autorisation pour supprimer un collaboration existante	Écrire	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConfiguredAudienceModelAssociation	Octroie l'autorisation de supprimer une association de modèles d'audience configurés existante.	Écrire	configuredaudiencemodelassociation*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteConfiguredTable	Accorde l'autorisation pour supprimer un tableau configuré	Écrire	configuredtable*		
DeleteConfiguredTableAnalysisRule	Accorde l'autorisation de supprimer une règle d'analyse existante	Écrire	configuredtable*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConfiguredTableAssociation	Accorde l'autorisation de supprimer une association de tableaux configurés d'une collaboration	Écrire	configuredtableassociation*		
DeleteConfiguredTableAssociationAnalysisRule	Autorise la suppression d'une règle d'analyse d'association de tables configurée existante	Écrire	configuredtableassociation*		
DeleteIdMappingTable	Accorde l'autorisation de supprimer une table de mappage d'identifiants d'une collaboration	Écrire	idmappingtable*		entityresolution:DeletePolicyStatement
			membership*		
DeleteIdNamespaceAssociation	Accorde l'autorisation de supprimer une association d'espaces de noms Id d'une collaboration	Écrire	idnamespaceassociation*		entityresolution:DeletePolicyStatement
			membership*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteMember	Accorde l'autorisation de supprimer des membres d'une collaboration	Écrire	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteMembership	Accorde l'autorisation de quitter les collaborations en supprimant une adhésion	Écrire	membership*		
DeletePrivacyBudgetTemplate	Octroie l'autorisation de supprimer un modèle budgétaire de confidentialité existant.	Écrire	privacybudgettemplate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAnalysisTemplate	Octroie l'autorisation d'afficher les détails d'un modèle d'analyse.	Lecture	analysistemplate*		
GetCollaboration	Accorde l'autorisation d'afficher les détails d'une collaboration	Lecture	collaboration*		
GetCollaborationAnalysisTemplate	Octroie l'autorisation d'afficher les détails d'un modèle d'analyse au sein d'une collaboration.	Lecture	analysistemplate*		
			collaboration*		
GetCollaborationChangeRequest	Accorde l'autorisation d'obtenir une demande de modification dans le cadre d'une collaboration	Lecture	collaboration*		
GetCollaborationConfiguredAudienceModelAssociation	Octroie l'autorisation d'afficher les détails d'une association de modèles d'audience configurés au sein d'une collaboration.	Lecture	collaboration*		
			configuredaudiencemodelassociation*		
GetCollaborationIdNamespaceAssociation	Accorde l'autorisation d'obtenir l'association d'espaces de noms d'identifiant au sein d'une collaboration	Lecture	collaboration*		
			idnamespaceassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCollaborationPrivacyBudgetTemplate	Octroie l'autorisation d'afficher les détails d'un modèle budgétaire de confidentialité au sein d'une collaboration.	Lecture	collaboration*		
			privacybudgettemplate*		
GetConfiguredAudienceModelAssociation	Octroie l'autorisation d'afficher les détails d'une association de modèles d'audience configurés.	Lecture	configuredaudiencemodelassociation*		
GetConfiguredTable	Accorde l'autorisation d'afficher les détails d'un tableau configuré	Lecture	configuredtable*		
GetConfiguredTableAnalysisRule	Accorde l'autorisation d'afficher les règles d'analyse pour un tableau configuré	Lecture	configuredtable*		
GetConfiguredTableAssociation	Accorde l'autorisation d'afficher les détails d'une association de tableaux configurés	Lecture	configuredtableassociation*		
GetConfiguredTableAssociationAnalysisRule	Accorde l'autorisation de consulter les règles d'analyse pour une association de tables configurée	Lecture	configuredtableassociation*		
GetIdMappingTable	Accorde l'autorisation d'afficher les détails d'une table de mappage d'identifiants	Lecture	idmappingtable*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			membership*		
GetIdNamespaceAssociation	Accorde l'autorisation d'afficher les détails d'une association d'espaces de noms d'identification	Lecture	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		
GetMembership	Accorde l'autorisation d'afficher les informations sur une adhésion	Lecture	membership*		
GetPrivacyBudgetTemplate	Octroie l'autorisation d'afficher les détails d'un modèle budgétaire de confidentialité.	Lecture	privacybudgettemplate*		
GetProtectedJob	Accorde l'autorisation de consulter une offre d'emploi protégée	Lecture	membership*		
GetProtectedQuery	Accorde l'autorisation d'afficher une requête protégée	Lecture	membership*		
GetSchema	Accorde l'autorisation d'afficher les détails d’un schéma	Lecture	collaboration*		
			configuredtableassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSchemaAnalysisRule	Accorde l'autorisation d'afficher les règles d'analyse associées à un schéma	Lecture	collaboration*		cleanrooms:GetSchema
			configuredtableassociation*		
ListAnalysisTemplates	Octroie l'autorisation de répertorier les modèles d'analyse disponibles.	List	analysistemplate*		
			membership*		
ListCollaborationAnalysisTemplates	Octroie l'autorisation de répertorier les modèles d'analyse disponibles au sein d'une collaboration.	List	collaboration*		
ListCollaborationChangeRequests	Accorde l'autorisation de répertorier les demandes de modification dans une collaboration	List	collaboration*		
ListCollaborationConfiguredAudienceModelAssociations	Octroie l'autorisation de répertorier les associations de modèles d'audience configurés disponibles au sein d'une collaboration.	List	collaboration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCollaborationIdNamespaceAssociations	Accorde l'autorisation de répertorier les espaces de noms d'identifiants au sein d'une collaboration	List	collaboration*		
ListCollaborationPrivacyBudgetTemplates	Octroie l'autorisation de répertorier les modèles budgétaires de confidentialité disponibles au sein d'une collaboration.	List	collaboration*		
ListCollaborationPrivacyBudgets	Octroie l'autorisation de répertorier les budgets de confidentialité au sein d'une collaboration.	List	collaboration*		
ListCollaborations	Accorde l'autorisation de répertorier les collaborations disponibles	List			
ListConfiguredAudienceModelAssociations	Octroie l'autorisation de répertorier les associations de modèles d'audience configurés disponibles pour une adhésion.	List	configuredaudiencemodelassociation* membership*		
ListConfiguredTableAssociations	Accorde l'autorisation de répertorier les associations de tableaux configurés disponibles pour une adhésion	List	configuredtableassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			membership*		
ListConfiguredTables	Accorde l'autorisation de répertorier les tableaux configurés disponibles	List			
ListIdMappingTables	Accorde l'autorisation de répertorier les tables de mappage d'identifiants disponibles pour un membre	List	idmappingtable*		
			membership*		
ListIdNamespaceAssociations	Autorise un membre à répertorier les associations de données de résolution d'entités	List	idnamespaceassociation*		
			membership*		
ListMembers	Accorde l'autorisation de répertorier les membres d'une collaboration	List	collaboration*		
ListMemberships	Accorde l'autorisation de répertorier les adhésions disponibles	List			
ListPrivacyBudgetTemplates	Octroie l'autorisation de répertorier les modèles budgétaires de confidentialité disponibles.	List	membership*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			privacybudgettemplate*		
ListPrivacyBudgets	Octroie l'autorisation de répertorier les budgets de confidentialité disponibles.	List	membership*		
ListProtectedJobs	Donne l'autorisation de répertorier les emplois protégés	List	membership*		
ListProtectedQueries	Accorde l'autorisation d'émettre des requêtes protégées	List	membership*		
ListSchemas	Accorde l'autorisation d'afficher les schémas disponibles pour une collaboration	List	collaboration*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource.	Liste	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			configuredtableassociation		
			membership		
			privacybudgettemplate		
PassCollaboration [autorisation uniquement]	Accorde l'autorisation d'accéder à une collaboration dans le contexte des modèles personnalisés de Clean Rooms ML	Lecture	collaboration*		
PassMembership [autorisation uniquement]	Accorde l'autorisation d'accéder à un abonnement dans le contexte des modèles personnalisés de Clean Rooms ML	Lecture	membership*		
PopulateIdMappingTable	Accorde l'autorisation de démarrer un Job de mappage d'identifiants dans AWS Entity Resolution afin de générer des résultats de mappage d'identifiants dans le cadre d'une collaboration en salles blanches.	Écrire	idmappingtable*		entityresolution:GetIdMappingWorkflow
			membership*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PreviewPrivacyImpact	Octroie l'autorisation de prévisualiser les paramètres du modèle budgétaire de confidentialité.	Lecture	membership*		
StartProtectedJob	Donne l'autorisation de créer des emplois protégés	Écrire	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema
			analysistemplate		
			configuredtableassociation		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartProtectedQuery	Accorde l'autorisation de lancer des requêtes protégées	Écrire	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema s3:GetBucketLocation s3:ListBucket s3:PutObject
			analysistemplate		
			configuredtableassociation		
			idmappingtable		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	analysistemplate		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		
			privacybudgettemplate		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			membership		
			privacybudgettemplate		
				aws:TagKeys	
UpdateAnalysisTemplate	Octroie l'autorisation de mettre à jour les détails du modèle d'analyse.	Écrire	analysistemplate*		
UpdateCollaboration	Accorde l'autorisation de mettre à jour les détails de la collaboration	Écrire	collaboration*		
UpdateCollaborationChangeRequest	Accorde l'autorisation de mettre à jour une demande de modification dans une collaboration	Écrire	collaboration*		
UpdateConfiguredAudienceModelAssociation	Octroie l'autorisation de mettre à jour une association de modèles d'audience configurés.	Écrire	configuredaudiencemodelassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConfiguredTable	Accorde l'autorisation de mette à jour un tableau configuré existant	Écrire	configuredtable*		athena:GetTableMetadata cleanrooms:UpdateConfiguredTableAllowedColumns cleanrooms:UpdateConfiguredTableReference glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					glue:GetSchemaVersion glue:GetTable glue:GetTables
UpdateConfiguredTableAllowedColumns [autorisation uniquement]	Accorde l'autorisation de mettre à jour les colonnes autorisées d'une table configurée existante	Écrire	configuredtable*		
UpdateConfiguredTableAnalysisRule	Accorde l'autorisation de mettre à jour les règles d'analyse d'un tableau configuré	Écrire	configuredtable*		
UpdateConfiguredTableAssociation	Accorde l'autorisation de mettre à jour une association configurée	Écrire	configuredtableassociation*		iam:PassRole
UpdateConfiguredTableAssociationAnalysisRule	Accorde l'autorisation de mettre à jour les règles d'analyse pour une association de tables configurée	Écrire	configuredtableassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConfiguredTableReference [autorisation uniquement]	Accorde l'autorisation de mettre à jour la référence de table d'une table configurée existante	Écrire	configuredtable*		
UpdateIdMappingTable	Accorde l'autorisation de mettre à jour une table de mappage d'identifiants	Écrire	idmappingtable*		
			membership*		
UpdateIdNamespaceAssociation	Autorise la mise à jour d'une association d'entrée de résolution d'entité	Écrire	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMembership	Accorde l'autorisation de mettre à jour les informations relatives à une adhésion	Écrire	membership*		iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
UpdatePrivacyBudgetTemplate	Octroie l'autorisation de mettre à jour les détails du modèle budgétaire de confidentialité.	Écrire	privacybudgettemplate*		
UpdateProtectedJob	Donne l'autorisation de mettre à jour les emplois protégés	Écrire	membership*		
UpdateProtectedQuery	Accorde l'autorisation de mettre à jour les requêtes protégées	Écrire	membership*		

Types de ressources définis par AWS Clean Rooms

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
analysistemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/analysistemplate/${AnalysisTemplateId}	aws:ResourceTag/${TagKey}
collaboration	arn:${Partition}:cleanrooms:${Region}:${Account}:collaboration/${CollaborationId}	aws:ResourceTag/${TagKey}
configuredaudiencemodelassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredaudiencemodelassociation/${ConfiguredAudienceModelAssociationId}	aws:ResourceTag/${TagKey}
configuredtable	arn:${Partition}:cleanrooms:${Region}:${Account}:configuredtable/${ConfiguredTableId}	aws:ResourceTag/${TagKey}
configuredtableassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredtableassociation/${ConfiguredTableAssociationId}	aws:ResourceTag/${TagKey}
idmappingtable	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idmappingtable/${IdMappingTableId}	aws:ResourceTag/${TagKey}
idnamespaceassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idnamespaceassociation/${IdNamespaceAssociationId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
membership	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}	aws:ResourceTag/${TagKey}
privacybudgettemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/privacybudgettemplate/${PrivacyBudgetTemplateId}	aws:ResourceTag/${TagKey}

Clés d'état pour les salles AWS propres

AWS Clean Rooms définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Clean Rooms ML

AWS Clean Rooms ML (préfixe de service :`cleanrooms-ml`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Clean Rooms ML
- Types de ressources définis par AWS Clean Rooms ML
- Clés de condition pour AWS Clean Rooms ML

Actions définies par AWS Clean Rooms ML

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelTrainedModel	Autorise l'annulation d'un modèle entraîné	Écrire	TrainedModel*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CancelTrainedModelInferenceJob	Autorise l'annulation d'une tâche d'inférence de modèles entraînés	Écrire	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAudienceModel	Octroie l'autorisation de créer un modèle d'audience.	Écrire	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredAudienceModel	Octroie l'autorisation de créer un modèle d'audience configuré.	Écrire	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfiguredModelAlgorithm	Accorde l'autorisation de créer un algorithme de modèle configuré	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredModelAlgorithmAssociation	Accorde l'autorisation de créer une association d'algorithmes de modèle configurée	Écrire	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMLInputChannel	Accorde l'autorisation de créer un canal d'entrée ML	Écrire	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTrainedModel	Autorise la création d'un modèle entraîné	Écrire	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainingDataset	Octroie l'autorisation de créer un jeu de données d'entraînement ou une audience de démarrage. Dans Clean Rooms ML, TrainingDataset il s'agit de métadonnées qui pointent vers une table Glue, qui est en lecture seule lors de AudienceModel la création	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceGenerationJob	Octroie l'autorisation de supprimer la tâche de génération d'audience spécifiée et supprime toutes les données associées à la tâche.	Écrire	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAudienceModel	Octroie l'autorisation de supprimer la tâche de génération d'audience spécifiée et supprime toutes les données associées à la tâche.	Écrire	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModel	Octroie l'autorisation de supprimer le modèle d'audience configuré spécifié.	Écrire	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModelPolicy	Octroie l'autorisation de supprimer la politique du modèle d'audience configuré spécifié.	Écrire	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConfiguredModelAlgorithm	Accorde l'autorisation de supprimer un algorithme de modèle configuré	Écrire	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithmAssociation	Accorde l'autorisation de supprimer une association d'algorithme de modèle configurée	Écrire	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLConfiguration	Accorde l'autorisation de supprimer une configuration ML	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLInputChannelData	Autorise la suppression de toutes les données associées au canal d'entrée ML	Écrire	MLInputChannel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainedModelOutput	Accorde l'autorisation de supprimer toutes les sorties associées au modèle entraîné	Écrire	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainingDataset	Octroie l'autorisation de supprimer un jeu de données d'entraînement.	Écrire	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceGenerationJob	Octroie l'autorisation de renvoyer des informations sur une tâche de génération d'audience.	Lecture	audiencegenerationjob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceModel	Octroie l'autorisation de renvoyer des informations sur un modèle d'audience.	Lecture	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCollaborationConfiguredModelAlgorithmAssociation	Accorde l'autorisation de renvoyer des informations sur une association d'algorithmes de modèle configurée créée par n'importe quel membre de la collaboration	Lecture	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCollaborationMLInputChannel	Accorde l'autorisation de renvoyer des informations sur un canal d'entrée ML créé par n'importe quel membre de la collaboration	Lecture	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetCollaborationTrainedModel	Accorde l'autorisation de renvoyer des informations sur un modèle entraîné créé par n'importe quel membre de la collaboration	Lecture	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConfiguredAudienceModel	Octroie l'autorisation de renvoyer des informations sur un modèle d'audience configuré.	Lecture	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredAudienceModelPolicy	Octroie l'autorisation de renvoyer des informations sur une politique de modèle d'audience configuré.	Lecture	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithm	Accorde l'autorisation de renvoyer des informations sur un algorithme de modèle configuré	Lecture	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConfiguredModelAlgorithmAssociation	Accorde l'autorisation de renvoyer des informations sur une association d'algorithmes de modèle configurée	Lecture	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetMLConfiguration	Accorde l'autorisation de renvoyer des informations sur une configuration ML	Lecture		aws:RequestTag/${TagKey} aws:TagKeys	
GetMLInputChannel	Accorde l'autorisation de renvoyer des informations sur un canal d'entrée ML	Lecture	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModel	Donne l'autorisation de renvoyer des informations sur un modèle entraîné	Lecture	TrainedModel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModelInferenceJob	Accorde l'autorisation de renvoyer des informations sur une tâche d'inférence de modèles entraînée	Lecture	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainingDataset	Octroie l'autorisation de renvoyer des informations sur un jeu de données d'entraînement.	Lecture	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceExportJobs	Octroie l'autorisation de renvoyer une liste des tâches d'exportation d'audience.	List	audiencegeneration job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceGenerationJobs	Octroie l'autorisation de renvoyer une liste des tâches de génération d'audience.	List	configuredaudiencemodel		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceModels	Octroie l'autorisation de renvoyer une liste des modèles d'audience.	List			
ListCollaborationConfiguredModelAlgorithmAssociations	Accorde l'autorisation de renvoyer une liste d'algorithmes de modèles configurés créés par n'importe quel membre de la collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCollaborationMLInputChannels	Accorde l'autorisation de renvoyer une liste de canaux d'entrée ML créés par n'importe quel membre de la collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModelExportJobs	Accorde l'autorisation de renvoyer une liste de jobs d'exportation modèles formés créés par n'importe quel membre de la collaboration	List	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCollaborationTrainedModelInferenceJobs	Accorde l'autorisation de renvoyer une liste de tâches d'inférence de modèles entraînées lancées par n'importe quel membre de la collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModels	Accorde l'autorisation de renvoyer une liste de modèles entraînés créés par n'importe quel membre de la collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListConfiguredAudienceModels	Octroie l'autorisation de renvoyer une liste des modèles d'audience configurés.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConfiguredModelAlgorithmAssociations	Autorise le renvoi d'une liste d'associations d'algorithmes de modèles configurées	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListConfiguredModelAlgorithms	Autorise le renvoi d'une liste d'algorithmes de modèles configurés	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListMLInputChannels	Autorise le renvoi d'une liste de canaux d'entrée ML	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListTagsForResource	Octroie l'autorisation de renvoyer une liste de balises pour une ressource fournie.	List	audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
ListTrainedModelInferenceJobs	Autorise le renvoi d'une liste de tâches d'inférence de modèles entraînées	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModelVersions	Autorise le renvoi d'une liste de versions de modèles entraînées	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModels	Autorise le renvoi d'une liste de modèles entraînés	List		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTrainingDatasets	Octroie l'autorisation de renvoyer une liste de jeux de données d'entraînement.	List			
PutConfiguredAudienceModelPolicy	Octroie l'autorisation de créer ou de mettre à jour la politique de ressource d'un modèle d'audience configuré.	Gestion des autorisations	configuredaudiencemodel*		
PutMLConfiguration	Accorde l'autorisation de mettre une configuration ML	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceExportJob	Octroie l'autorisation d'exporter une audience d'une taille spécifiée après avoir généré une audience.	Écrire	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceGenerationJob	Octroie l'autorisation de démarrer la tâche de génération d'audience.	Écrire	configuredaudiencemodel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
StartTrainedModelExportJob	Donne l'autorisation de créer un poste d'exportation modèle formé	Écrire	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartTrainedModelInferenceJob	Donne l'autorisation de démarrer une tâche d'inférence de modèles entraînée	Écrire	ConfiguredModelAlgorithmAssociation*		
			MLInputChannel*		
			TrainedModel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Octroie l'autorisation de baliser une ressource spécifique.	Identification	ConfiguredModelAlgorithm		
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnTagResource	Octroie l'autorisation d'annuler le balisage d'une ressource spécifique.	Identification	ConfiguredModelAlgorithm		
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConfiguredAudienceModel	Octroie l'autorisation de mettre à jour un modèle d'audience configuré.	Écrire	configuredaudiencemodel*		
			audiencemodel		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	

Types de ressources définis par AWS Clean Rooms ML

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
trainingdataset	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:training-dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
audiencemodel	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-model/${ResourceId}`	aws:ResourceTag/${TagKey}
configuredaudiencemodel	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-audience-model/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
audiencegenerationjob	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-generation-job/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithm	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-model-algorithm/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithmAssociation	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/configured-model-algorithm-association/${ResourceId}	aws:ResourceTag/${TagKey}
MLInputChannel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/ml-input-channel/${ResourceId}	aws:ResourceTag/${TagKey}
TrainedModel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model/${ResourceId}	aws:ResourceTag/${TagKey}
TrainedModelInferenceJob	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model-inference-job/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Clean Rooms ML

AWS Clean Rooms ML définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
cleanrooms-ml:CollaborationId	Filtre l'accès par identifiant de collaboration pour les salles propres	String

Actions, ressources et clés de condition pour l'API AWS Cloud de contrôle

AWS Cloud L'API de contrôle (préfixe de service :`cloudformation`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'API AWS Cloud de contrôle
- Types de ressources définis par l'API AWS Cloud de contrôle
- Clés de condition pour l'API AWS Cloud de contrôle

Actions définies par l'API AWS Cloud de contrôle

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelResourceRequest	Accorde l'autorisation d'annuler des demandes de ressources dans votre compte	Écrire			
CreateResource	Accorde l'autorisation de créer des ressources dans votre compte	Écrire			
DeleteResource	Accorde l'autorisation de supprimer des ressources dans votre compte	Écrire			
GetResource	Accorde l'autorisation d'obtenir des ressources dans votre compte	Lecture			
GetResourceRequestStatus	Accorde l'autorisation d'obtenir des demandes de ressources dans votre compte	Lecture			
ListResourceRequests	Accorde l'autorisation de répertorier des demandes de ressources dans votre compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResources	Accorde l'autorisation de répertorier des ressources dans votre compte	Lecture			
UpdateResource	Accorde l'autorisation de mettre à jour des ressources dans votre compte	Écrire			

Types de ressources définis par l'API AWS Cloud de contrôle

AWS Cloud L'API de contrôle ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à l'API AWS Cloud Control, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour l'API AWS Cloud de contrôle

L'API Cloud Control ne comporte pas de clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Cloud Directory

Amazon Cloud Directory (préfixe de service : `clouddirectory`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Cloud Directory
- Types de ressources définis par Amazon Cloud Directory
- Clés de condition pour Amazon Cloud Directory

Actions définies par Amazon Cloud Directory

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddFacetToObject	Accorde l'autorisation d'ajouter une nouvelle facette à un objet.	Écrire	directory*		
ApplySchema	Accorde l'autorisation de copier le schéma publié d'entrée dans le répertoire avec les mêmes nom et version que ceux du schéma publié.	Écrire	directory* publishedSchema*		
AttachObject	Accorde l'autorisation d'attacher un objet existant à un autre objet existant.	Écrire	directory*		
AttachPolicy	Accorde l'autorisation d'attacher un objet de politique à n'importe quel autre objet.	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AttachToIndex	Accorde l'autorisation d'attacher l'objet spécifié à l'index spécifié.	Écrire	directory*		
AttachTypedLink	Accorde l'autorisation de joindre un lien saisi à b/w une référence à un objet source et cible	Écrire	directory*		
BatchRead	Accorde l'autorisation d'effectuer toutes les opérations de lecture dans un lot. Chaque opération individuelle à l'intérieur BatchRead doit recevoir des autorisations explicites	Lecture	directory*		
BatchWrite	Accorde l'autorisation d'effectuer toutes les opérations d'écriture dans un lot. Chaque opération individuelle à l'intérieur BatchWrite doit recevoir des autorisations explicites	Écrire	directory*		
CreateDirectory	Accorde l'autorisation de créer un répertoire en copiant le schéma publié dans le répertoire.	Écrire	publishedSchema*		
CreateFacet	Accorde l'autorisation de créer une nouvelle facette dans un schéma.	Écrire	appliedSchema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			developmentSchema*		
CreateIndex	Accorde l'autorisation de créer un objet d'index.	Écrire	directory*		
CreateObject	Accorde l'autorisation de créer un objet dans le répertoire.	Écrire	directory*		
CreateSchema	Accorde l'autorisation de créer nouveau schéma dans un état de développement.	Écrire			
CreateTypedLinkFacet	Accorde l'autorisation de créer une nouvelle facette de lien saisi dans un schéma.	Écrire	appliedSchema*		
			developmentSchema*		
DeleteDirectory	Accorde l'autorisation de supprimer un répertoire. Seuls les répertoires désactivés peuvent être supprimés.	Écrire	directory*		
DeleteFacet	Accorde l'autorisation de supprimer une facette donnée. Tous les attributs et règles associés à la facette seront supprimés.	Écrire	developmentSchema*		
DeleteObject	Accorde l'autorisation de supprimer un objet et ses attributs associés.	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSchema	Accorde l'autorisation de supprimer un schéma donné.	Écrire	developmentSchema*		
			publishedSchema*		
DeleteTypedLinkFacet	Accorde l'autorisation de supprimer une TypedLink facette donnée. Tous les attributs et règles associés à la facette seront supprimés.	Écrire	developmentSchema*		
DetachFromIndex	Accorde l'autorisation de détacher l'objet spécifié de l'index spécifié.	Écrire	directory*		
DetachObject	Accorde l'autorisation de détacher un objet donné de l'objet parent.	Écrire	directory*		
DetachPolicy	Accorde l'autorisation de détacher une politique d'un objet.	Écrire	directory*		
DetachTypedLink	Accorde l'autorisation de détacher un lien b/w typé donné en fonction de la source et de la référence de l'objet cible	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableDirectory	Accorde l'autorisation de désactiver le répertoire spécifié.	Écrire	directory*		
EnableDirectory	Accorde l'autorisation d'activer le répertoire spécifié.	Écrire	directory*		
GetAppliedSchemaVersion	Accorde l'autorisation de renvoyer la version actuelle du schéma ARN appliqué, y compris la version mineure utilisée	Lecture	appliedSchema*		
GetDirectory	Accorde l'autorisation de récupérer des métadonnées d'un répertoire.	Lecture	directory*		
GetFacet	Accorde l'autorisation d'obtenir les détails de la facette, tels que le nom de la facette, les attributs, les règles ou ObjectType	Lecture	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetLinkAttributes	Accorde l'autorisation de récupérer des attributs associés à un lien saisi.	Lecture	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetObjectAttributes	Accorde l'autorisation de récupérer les attributs au sein d'une facette qui sont associés à un objet.	Lecture	directory*		
GetObjectInformation	Accorde l'autorisation de récupérer les métadonnées d'un objet.	Lecture	directory*		
GetSchemaAsJson	Accorde l'autorisation de récupérer une représentation JSON du schéma.	Lecture	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetTypedLinkFacetInformation	Accorde l'autorisation de renvoyer les informations d'ordre des attributs d'identité associées à une facette de lien saisi donnée.	Lecture	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListAppliedSchemaArns	Accorde l'autorisation de répertorier les schémas appliqués à un répertoire.	List	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAttachedIndices	Accorde l'autorisation de répertorier les indices attachés à un objet.	Lecture	directory*		
ListDevelopmentSchemaArns	Accorde l'autorisation ARNs de récupérer les schémas dans l'état de développement	List			
ListDirectories	Accorde l'autorisation de répertorier les répertoires créés dans un compte.	List			
ListFacetAttributes	Accorde l'autorisation de récupérer les attributs attachés à la facette.	Lecture	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListFacetNames	Accorde l'autorisation de récupérer les noms des facettes existant dans un schéma.	Lecture	appliedSchema*		
			developmentSchema*		
			publishedSchema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIncomingTypedLinks	Accorde l'autorisation de renvoyer une liste paginée de toutes les entrées TypedLinks pour un objet donné	Lecture	directory*		
ListIndex	Accorde l'autorisation de répertorier les objets attachés à l'index spécifié.	Lecture	directory*		
ListManagedSchemaArns	Accorde l'autorisation de répertorier les familles de versions majeures de chaque schéma géré. Si un ARN de version majeure est fourni en tant que SchemaArn, les révisions des versions mineures de cette famille sont répertoriées à la place	List			
ListObjectAttributes	Accorde l'autorisation de répertorier tous les attributs associés à un objet.	Lecture	directory*		
ListObjectChildren	Accorde l'autorisation de renvoyer une liste paginée des objets enfants associés à un objet donné.	Lecture	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListObjectParentPaths	Accorde l'autorisation de récupérer tous les chemins parents disponibles pour tous les types d'objets, tels que les objets de nœud, de nœud secondaire, de politique ou d'index.	Lecture	directory*		
ListObjectParents	Accorde l'autorisation de répertorier les objets parents associés à un objet donné sous forme de pagination.	Lecture	directory*		
ListObjectPolicies	Accorde l'autorisation de renvoyer les politiques attachées à un objet sous forme de pagination.	Lecture	directory*		
ListOutgoingTypedLinks	Accorde l'autorisation de renvoyer une liste paginée de toutes les données sortantes TypedLinks pour un objet donné	Lecture	directory*		
ListPolicyAttachments	Accorde l'autorisation de renvoyer tous les ObjectIdentifiers éléments auxquels une politique donnée est attachée	Lecture	directory*		
ListPublishedSchemaArns	Accorde l'autorisation de récupérer le schéma publié ARNs	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de renvoyer des étiquettes pour une ressource.	Lecture	directory*		
ListTypedLinkFacetAttributes	Accorde l'autorisation de renvoyer une liste paginée des attributs associés à la facette de lien saisi.	Lecture	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListTypedLinkFacetNames	Accorde l'autorisation de renvoyer une liste paginée des noms de facettes de lien saisi qui existent dans un schéma.	Lecture	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
LookupPolicy	Accorde l'autorisation de répertorier toutes les politiques de la racine du répertoire jusqu'à l'objet spécifié.	Lecture	directory*		
PublishSchema	Accorde l'autorisation de publier un schéma de développement avec une version.	Écrire	developmentSchema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutSchemaFromJson	Accorde l'autorisation de mettre à jour un schéma à l'aide du chargement JSON. Disponible uniquement pour les schémas de développement.	Écrire			
RemoveFacetFromObject	Accorde l'autorisation de supprimer la facette spécifiée de l'objet spécifié.	Écrire	directory*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	directory*		
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	directory*		
UpdateFacet	Accorde l'autorisation aux attributs, aux règles ou à ObjectType une facette add/update/delete existants	Écrire	appliedSchema*		
			developmentSchema*		
UpdateLinkAttributes	Accorde l'autorisation de mettre à jour les attributs d'un lien saisi donné. Les attributs à mettre à jour ne doivent pas contribuer à l'identité du lien saisi, telle que définie par son IdentityAttributeOrder	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateObjectAttributes	Accorde l'autorisation de mettre à jour les attributs d'un objet donné.	Écrire	directory*		
UpdateSchema	Accorde l'autorisation de mettre à jour le nom du schéma avec un nouveau nom.	Écrire	developmentSchema*		
UpdateTypedLinkFacet	Accorde l'autorisation aux attributs add/update/delete existants, aux règles, à l'ordre des attributs d'identité d'une TypedLink facette	Écrire	developmentSchema*		
UpgradeAppliedSchema	Accorde l'autorisation de mettre à niveau un seul répertoire sur place à l'aide des PublishedSchemaArn mises à jour de schéma trouvées dans MinorVersion. Les mises à niveau des versions mineures rétrocompatibles sont instantanément disponibles pour les lecteurs sur tous les objets du répertoire.	Écrire	directory* publishedSchema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpgradePublishedSchema	Autorise la mise à niveau d'un schéma publié dans le cadre d'une nouvelle révision de version mineure en utilisant le contenu actuel de DevelopmentSchemaArn	Écrire	developmentSchema*		
			publishedSchema*		

Types de ressources définis par Amazon Cloud Directory

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
appliedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}/schema/${SchemaName}/${Version}`	
developmentSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/development/${SchemaName}`	

Types de ressources	ARN	Clés de condition
directory	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}`	
published Schema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/published/${SchemaName}/${Version}`	

Clés de condition pour Amazon Cloud Directory

Cloud Directory ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Cloud la carte

AWS Cloud La carte (préfixe de service :`servicediscovery`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Cloud la carte
- Types de ressources définis par AWS Cloud la carte
- Clés de condition pour AWS Cloud la carte

Actions définies par AWS Cloud la carte

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateHttpNamespace	Accorde l'autorisation de créer un espace de noms HTTP	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePrivateDnsNamespace	Accorde l'autorisation de créer un espace de noms privé basé sur DNS, qui sera visible uniquement dans un VPC Amazon spécifié	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePublicDnsNamespace	Accorde l'autorisation de créer un espace de noms public basé sur DNS, qui sera visible sur Internet	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Accorde l'autorisation de créer un service	Écriture	namespace* service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				servicediscovery:NamespaceArn aws:TagKeys aws:RequestTag/${TagKey}	
DeleteNamespace	Accorde l'autorisation de supprimer un espace de noms spécifié	Écrire	namespace*		
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer la politique de contrôle d'accès à la RAM pour un espace de noms	Écrire	namespace*		
DeleteService	Accorde l'autorisation de supprimer un service spécifié	Écrire	service*		
				servicediscovery:ServiceCreatedByAccount	
DeleteServiceAttributes	Accorde l'autorisation de supprimer des attributs spécifiés d'un service	Écrire	service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				servicediscovery:ServiceCreatedByAccount	
DeregisterInstance	Accorde l'autorisation de supprimer les enregistrements et la vérification de l'état, le cas échéant, créés par Amazon Route 53 pour l'instance spécifiée	Écriture	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
DiscoverInstances	Accorde l'autorisation de découvrir les instances enregistrées pour un espace de noms et un service spécifiés	Lecture	namespace*		
			service*		
				servicediscovery:NamespaceName servicediscovery:ServiceName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DiscoverInstancesRevision	Accorde l'autorisation de découvrir la révision des instances pour un espace de noms et un service spécifiés	Lecture	namespace*		
			service*		
				servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	Accorde l'autorisation d'obtenir des informations sur une instance spécifiée	Lecture	service*		
				servicediscovery:ServiceArn	
GetInstancesHealthStatus	Accorde l'autorisation d'obtenir l'état d'intégrité actuel (Sain, Non sain ou Inconnu) d'une ou de plusieurs instances	Lecture	service*		
				servicediscovery:ServiceArn	
GetNamespace	Accorde l'autorisation d'obtenir des informations sur un espace de noms	Lecture	namespace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOperation	Accorde l'autorisation d'obtenir des informations sur une opération spécifique	Lecture	namespace*		
			service		
GetResourcePolicy [autorisation uniquement]	Accorde l'autorisation de lire la politique de contrôle d'accès à la RAM pour un espace de noms	Lecture	namespace*		
GetService	Accorde l'autorisation d'obtenir les paramètres d'un service spécifié	Lecture	service*		
GetServiceAttributes	Accorde l'autorisation d'obtenir les attributs d'un service spécifié	Lecture	service*		
ListInstances	Accorde l'autorisation d'obtenir des informations récapitulatives sur les instances qui ont été enregistrées auprès d'un service spécifié	Lecture	service*		
				servicediscovery:ServiceArn	
ListNamespaces	Accorde l'autorisation d'obtenir des informations sur les espaces de noms	Lecture			
ListOperations	Accorde l'autorisation de répertorier les opérations répondant aux critères que vous spécifiez	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServices	Accorde l'autorisation d'obtenir les paramètres pour tous les services qui correspondent aux filtres spécifiés	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises de la ressource spécifiée	Lecture			
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de définir la politique de contrôle d'accès à la RAM pour un espace de noms	Écrire	namespace*		
RegisterInstance	Accorde l'autorisation d'enregistrer une instance basée sur les paramètres d'un service spécifié	Écriture	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs identifications à la ressource spécifiée	Balisage		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises de la ressource spécifiée	Identification		aws:TagKeys	
UpdateHttpNamespace	Accorde l'autorisation de mettre à jour les paramètres d'un espace de noms HTTP	Écrire	namespace*		
UpdateInstanceCustomHealthStatus	Accorde l'autorisation de mettre à jour l'état d'intégrité actuel d'une instance qui possède une surveillance de l'état personnalisée	Écrire	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
UpdatePrivateDnsNamespace	Accorde l'autorisation de mettre à jour les paramètres d'un espace de noms DNS privé	Écrire	namespace*		
UpdatePublicDnsNamespace	Accorde l'autorisation de mettre à jour les paramètres d'un espace de noms DNS public	Écrire	namespace*		
UpdateService		Écrire	service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de mettre à jour les paramètres d'un service spécifié			servicediscovery:ServiceCreatedByAccount	
UpdateServiceAttributes	Accorde l'autorisation de mettre à jour les attributs dans un service spécifié	Écrire	service*		
				servicediscovery:ServiceCreatedByAccount	

Types de ressources définis par AWS Cloud la carte

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
namespace	`arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
service	`arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Cloud la carte

AWS Cloud La carte définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction des balises qui sont transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des balises associées à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction des clés de balise qui sont transmises dans la demande	ArrayOfString
servicediscovery:NamespaceArn	Filtre l'accès en spécifiant l'Amazon Resource Name (ARN) de l'espace de noms associé	ARN
servicediscovery:NamespaceName	Filtre l'accès en spécifiant le nom de l'espace de noms associé	Chaîne

Clés de condition	Description	Type
servicediscovery:ServiceArn	Filtre l'accès en spécifiant l'Amazon Resource Name (ARN) du service associé	ARN
servicediscovery:ServiceCreatedByAccount	Filtre l'accès en spécifiant l'identifiant de compte du créateur du service concerné	String
servicediscovery:ServiceName	Filtre l'accès en spécifiant le nom du service associé	String

Actions, ressources et clés de condition pour AWS Cloud9

AWS Cloud9 (préfixe de service :`cloud9`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Cloud9
- Types de ressources définis par AWS Cloud9
- Clés de condition pour AWS Cloud9

Actions définies par AWS Cloud9

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateEC2Remote [autorisation uniquement]	Accorde l'autorisation de démarrer l'instance Amazon EC2 à laquelle votre IDE AWS Cloud9 se connecte	Écrire	environment*		
CreateEnvironmentEC2	Accorde l'autorisation de créer un environnement de développement AWS Cloud9, lance une instance Amazon Elastic Compute Cloud (Amazon EC2), puis héberge l'environnement sur l'instance	Écrire		cloud9:EnvironmentName cloud9:InstanceType cloud9:SubnetId cloud9:UserArn cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEnvironmentMembership	Accorde l'autorisation d'ajouter un membre de l'environnement à un environnement de AWS développement Cloud9	Écrire	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
CreateEnvironmentSSH [autorisation uniquement]	Autorise la création d'un environnement de AWS développement Cloud9 SSH	Écrire		cloud9:EnvironmentName cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironmentToken [autorisation uniquement]	Accorde l'autorisation de créer un jeton d'authentification qui permet une connexion entre l'IDE AWS Cloud9 et l'environnement de l'utilisateur	Lecture	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEnvironment	Accorde l'autorisation de supprimer un AWS environnement de développement Cloud9. Si l'environnement est hébergé sur une instance Amazon Elastic Compute Cloud (Amazon EC2), met également fin à l'instance	Écrire	environment*		iam:CreateServiceLinkedRole
DeleteEnvironmentMembership	Accorde l'autorisation de supprimer un membre de l'environnement d'un environnement de AWS développement Cloud9	Écrire	environment*		
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEC2Remote [autorisation uniquement]	Accorde l'autorisation d'obtenir des détails sur la connexion à l'environnement de développement EC2, y compris l'hôte, l'utilisateur et le port	Lecture	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEnvironmentMemberships	Accorde l'autorisation d'obtenir des informations sur les membres de l'environnement pour un environnement de AWS développement Cloud9	Lecture	environment*		
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEnvironmentStatus	Accorde l'autorisation d'obtenir des informations de statut pour un environnement de AWS développement Cloud9	Lecture	environment*		
DescribeEnvironments	Accorde l'autorisation d'obtenir des informations sur les AWS environnements de développement Cloud9	Lecture	environment*		
DescribeSSHRemote [autorisation uniquement]	Accorde l'autorisation d'obtenir des détails sur la connexion à l'environnement de développement SSH, y compris l'hôte, l'utilisateur et le port	Lecture	environment*		
GetEnvironmentConfig [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations de configuration utilisées pour initialiser l'IDE AWS Cloud9	Lecture	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEnvironmentSettings [autorisation uniquement]	Accorde l'autorisation d'obtenir les paramètres de l'IDE AWS Cloud9 pour un environnement de développement spécifié	Lecture	environment*		
GetMembershipSettings [autorisation uniquement]	Accorde l'autorisation d'obtenir les paramètres de l'IDE AWS Cloud9 pour un membre de l'environnement spécifié	Lecture	environment*		
GetMigrationExperiences [autorisation uniquement]	Accorde l'autorisation d'obtenir l'expérience de migration pour un utilisateur Cloud9	Lecture			
GetUserPublicKey [autorisation uniquement]	Accorde l'autorisation d'obtenir la clé SSH publique de l'utilisateur, qui est utilisée par AWS Cloud9 pour se connecter aux environnements de développement SSH	Lecture		cloud9:UserArn	
GetUserSettings [autorisation uniquement]	Accorde l'autorisation d'obtenir les paramètres de l'IDE AWS Cloud9 pour un utilisateur spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEnvironments	Accorde l'autorisation d'obtenir une liste des identifiants de l' AWS environnement de développement Cloud9	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour un environnement Cloud9	Lecture	environment*		
ModifyTemporaryCredentialsOnEnvironmentEC2 [autorisation uniquement]	Accorde l'autorisation de définir des informations d'identification temporaires AWS gérées sur l'instance Amazon EC2 utilisée par l'environnement de développement intégré (AWS IDE) Cloud9	Écrire	environment*		
TagResource	Accorde l'autorisation d'ajouter des balises à un environnement Cloud9	Identification	environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises d'un environnement Cloud9	Identification	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateEnvironment	Autorise la modification des paramètres d'un environnement de développement AWS Cloud9 existant	Écrire	environment*		
UpdateEnvironmentMembership	Accorde l'autorisation de modifier les paramètres d'un membre d'environnement existant pour un environnement de AWS développement Cloud9	Écrire	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
UpdateEnvironmentSettings [autorisation uniquement]	Autorise la mise à jour des paramètres de l'IDE AWS Cloud9 pour un environnement de développement spécifié	Écrire	environment*		
UpdateMembershipSettings [autorisation uniquement]	Accorde l'autorisation de mettre à jour les paramètres de l'IDE AWS Cloud9 pour un membre de l'environnement spécifié	Écrire	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSSHRemote [autorisation uniquement]	Accorde l'autorisation de mettre à jour les détails sur la connexion à l'environnement de développement SSH, y compris l'hôte, l'utilisateur et le port	Écrire	environment*		
UpdateUserSettings [autorisation uniquement]	Accorde l'autorisation de mettre à jour les paramètres spécifiques à l'IDE d'un utilisateur Cloud9 AWS	Écrire			

Types de ressources définis par AWS Cloud9

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
environment	`arn:${Partition}:cloud9:${Region}:${Account}:environment:${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Cloud9

AWS Cloud9 définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
cloud9:EnvironmentId	Filtre l'accès en fonction de l'ID de l' AWS environnement Cloud9	String
cloud9:EnvironmentName	Filtre l'accès en fonction du nom de l' AWS environnement Cloud9	String
cloud9:InstanceType	Filtre l'accès en fonction du type d'instance de l'instance Amazon EC2 de l'environnement AWS Cloud9	String
cloud9:OwnerArn	Filtre l'accès en fonction de l'ARN du propriétaire spécifié	ARN
cloud9:Permissions	Filtre l'accès en fonction du type d' AWS autorisations Cloud9	String
cloud9:SubnetId	Filtre l'accès en fonction de l'ID de sous-réseau dans lequel l'environnement AWS Cloud9 sera créé	String

Clés de condition	Description	Type
cloud9:UserArn	Filtre l'accès en fonction de l'ARN utilisateur spécifié	ARN

Actions, ressources et clés de condition pour AWS CloudFormation

AWS CloudFormation (préfixe de service :`cloudformation`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CloudFormation
- Types de ressources définis par AWS CloudFormation
- Clés de condition pour AWS CloudFormation

Actions définies par AWS CloudFormation

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateOrganizationsAccess	Accorde l'autorisation d'activer un accès sécurisé entre StackSets et Organizations. Lorsque l'accès sécurisé est activé StackSets et que les Organisations sont activées, le compte de gestion dispose des autorisations nécessaires pour créer et gérer StackSets pour votre organisation.	Écrire			
ActivateType	Accorde l'autorisation d'activer une extension tierce publique, ce qui la rend disponible pour une utilisation dans les modèles de pile	Écrire			
BatchDescribeTypeConfigurations	Accorde l'autorisation de renvoyer les données de configuration pour les CloudFormation extensions spécifiées	Lecture			
CancelUpdateStack	Accorde l'autorisation d'annuler une mise à jour sur la pile spécifiée	Écriture	stack*		
ContinueUpdateRollback	Accorde l'autorisation de continuer à restaurer une pile qui se trouve dans l'état UPDATE_ROLLBACK_FA	Écriture	stack*		
				cloudformation:RoleArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	ILED vers l'état UPDATE_ROLLBACK_COMPLETE				
CreateChangeSet	Accorde l'autorisation de créer une liste de modifications pour une pile	Écrire	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				cloudformation:ChangeSetName cloudformation:ResourceTypes cloudformation:ImportResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateGeneratedTemplate	Accorde l'autorisation de créer un modèle à partir de ressources existantes qui ne sont pas déjà gérées avec CloudFormation	Écrire			
CreateStack	Accorde l'autorisation de créer une pile comme spécifié dans le modèle	Écriture	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateStackInstances	Accorde l'autorisation de créer des instances de piles pour les comptes spécifiés, dans les régions spécifiées	Écrire	stackset*		
			stackset-target		
			type		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys cloudformation:TargetRegion	
CreateStackRefactor	Accorde l'autorisation de créer un refactor de pile	Écrire	stack*		
CreateStackSet	Accorde l'autorisation de créer un ensemble de piles comme spécifié dans le modèle	Écriture		cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUploadBucket [autorisation uniquement]	Accorde l'autorisation de télécharger des modèles vers des compartiments Amazon S3 Utilisé uniquement par la AWS CloudFormation console et n'est pas documenté dans la référence de l'API	Écrire			
DeactivateOrganizationsAccess	Accorde l'autorisation de désactiver l'accès sécurisé entre StackSets et Organizations. Si l'accès sécurisé est désactivé, le compte de gestion n'est pas autorisé à créer et à gérer des services gérés pour votre StackSets organisation	Écrire			
DeactivateType	Accorde l'autorisation de désactiver une extension publique précédemment activée dans ce compte et cette région	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteChangeSet	Accorde l'autorisation de supprimer le jeu de modifications spécifié La suppression des jeux de modifications garantit que personne n'exécutera un jeu de modifications inapproprié	Écrire	stack*		
				cloudformation:ChangeSetName	
DeleteGeneratedTemplate	Accorde l'autorisation de supprimer un modèle généré	Écrire			
DeleteStack	Accorde l'autorisation de supprimer une pile spécifiée	Écriture	stack*		
				cloudformation:RoleArn	
DeleteStackInstances	Accorde l'autorisation de supprimer des instances de piles pour les comptes spécifiés, dans les régions spécifiées	Écriture	stackset*		
			stackset-target		
			type		
				cloudformation:TargetRegion	
DeleteStackSet	Accorde l'autorisation de supprimer un ensemble de piles spécifié	Écrire	stackset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterType	Accorde l'autorisation de désenregistrer un CloudFormation type ou une version de type existant	Écrire			
DescribeAccountLimits	Accorde l'autorisation de récupérer les AWS CloudFormation limites de votre compte	Lecture			
DescribeChangeSet	Accorde l'autorisation de renvoyer la description du jeu de modifications spécifié	Lecture	stack*		
				cloudformation:ChangeSetName	
DescribeChangeSetHooks	Accorde l'autorisation pour renvoyer les informations d'invocation Hook pour le jeu de modifications spécifié	Lecture	stack*		
				cloudformation:ChangeSetName	
DescribeEvents	Accorde l'autorisation de renvoyer tous les événements associés à une opération spécifiée	Lecture	changeset		
			stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGeneratedTemplate	Accorde l'autorisation de décrire un modèle généré. La sortie inclut des détails sur la progression de la création d'un modèle généré.	Lecture			
DescribeOrganizationsAccess	Accorde l'autorisation de renvoyer des informations sur le OrganizationAccess statut du compte	Lecture			
DescribePublisher	Accorde l'autorisation de renvoyer des informations sur CloudFormation l'éditeur d'une extension	Lecture			
DescribeResourceScan	Accorde l'autorisation de décrire les détails d'une analyse des ressources	Lecture			
DescribeStackDriftDetectionStatus	Accorde l'autorisation de renvoyer des informations sur une opération de détection de dérive de pile	Lecture			
DescribeStackEvents	Accorde l'autorisation de renvoyer tous les événements associés à une pile spécifiée	Lecture	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeStackInstance	Accorde l'autorisation de renvoyer l'instance de pile associée à l'ensemble de piles et à la région spécifiés Compte AWS	Lecture	stackset*		
DescribeStackRefactor	Accorde l'autorisation de renvoyer la description du refacteur de pile spécifié	Lecture	stack*		
DescribeStackResource	Accorde l'autorisation de renvoyer une description de la ressource spécifiée dans la pile spécifiée	Lecture	stack*		
DescribeStackResourceDrifts	Accorde l'autorisation de renvoyer les informations de dérive pour les ressources qui ont été vérifiées pour dérive dans la pile spécifiée	Lecture	stack*		
DescribeStackResources	Accorde l'autorisation de renvoyer les descriptions AWS des ressources pour les piles en cours d'exécution et supprimées	Lecture	stack*		
DescribeStackSet	Accorde l'autorisation de renvoyer la description de l'ensemble de piles spécifié	Lecture	stackset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeStackSetOperation	Accorde l'autorisation de renvoyer la description de l'opération de l'ensemble de piles spécifiée	Lecture	stackset*		
DescribeStacks	Accorde l'autorisation de renvoyer la description de la pile spécifiée et de toutes les piles lorsqu'elle est utilisée en combinaison avec l'action ListStacks	List	stack		cloudformation:ListStacks
DescribeType	Accorde l'autorisation de renvoyer des informations sur le CloudFormation type demandé	Lecture			
DescribeTypeRegistration	Accorde l'autorisation de renvoyer des informations sur le processus d'enregistrement pour un CloudFormation type	Lecture			
DetectStackDrift	Accorde l'autorisation de détecter si la configuration actuelle d'une pile diffère, ou a dérivé, de sa configuration attendue, telle que définie dans le modèle de pile, et des valeurs spécifiées comme paramètres du modèle	Lecture	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DetectStackResourceDrift	Accorde l'autorisation de renvoyer des informations permettant de savoir si la configuration actuelle d'une pile diffère, ou a dérivé, de sa configuration attendue, telle que définie dans le modèle de pile, et des valeurs spécifiées comme paramètres du modèle	Lecture	stack*		
DetectStackSetDrift	Accorde l'autorisation aux utilisateurs de détecter la dérive sur un ensemble de piles et les instances de piles qui appartiennent à cet ensemble de piles	Lecture	stackset*		
EstimateTemplateCost	Accorde l'autorisation de renvoyer le coût mensuel estimé d'un modèle	Lecture		cloudformation:TemplateUrl	
ExecuteChangeSet	Accorde l'autorisation de mettre à jour une pile à l'aide des informations d'entrée qui ont été fournies lorsque le jeu de modifications spécifié a été créé	Écrire	stack*		
				cloudformation:ChangeSetName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExecuteStackRefactor	Accorde l'autorisation d'exécuter un refactor de pile en utilisant les informations d'entrée fournies lors de la création du refactor de pile spécifié	Écrire	stack*		
GetGeneratedTemplate	Accorde l'autorisation de récupérer un modèle généré	Lecture			
GetHookResult	Accorde l'autorisation de renvoyer des informations détaillées sur le résultat d'un appel de hook spécifique	Lecture		cloudformation:TypeArn	kms:Decrypt
GetStackPolicy	Accorde l'autorisation de renvoyer la politique de pile d'une pile spécifiée	Lecture	stack*		
GetTemplate	Accorde l'autorisation de renvoyer le corps du modèle d'une pile spécifiée	Lecture	stack*		
GetTemplateSummary	Accorde l'autorisation de renvoyer des informations sur un modèle nouveau ou existant	Lecture	stack		
			stackset		
				cloudformation:TemplateUrl	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportStacksToStackSet	Accorde l'autorisation de permettre aux utilisateurs d'importer des piles existantes dans un ensemble de piles nouveau ou existant	Écrire	stackset*		
ListAllHookResults	Accorde l'autorisation de renvoyer les informations de résultat des invocations Hook pour un Hook spécifié, une combinaison de Hook et de statut, ou pour tous les Hooks	List		cloudformation:TypeArn	
ListChangeSets	Accorde l'autorisation de renvoyer l'ID et l'état de chaque jeu de modifications actif pour une pile. Par exemple, AWS CloudFormation répertorie les ensembles de modifications dont l'état est CREATE_IN_PROGRESS ou CREATE_PENDING	List	stack*		
ListExports	Accorde l'autorisation de répertorier toutes les valeurs de sortie exportées dans le compte et la région où vous appelez cette action	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGeneratedTemplates	Accorde l'autorisation de répertorier les modèles que vous avez générés dans cette région	List			
ListHookResults	Accorde l'autorisation de renvoyer les informations de résultat des invocations Hook pour la cible spécifiée	List	stack		
				cloudformation:ChangeSetName	
ListImports	Accorde l'autorisation de répertorier toutes les piles qui importent une valeur de sortie exportée	List			
ListResourceScanRelatedResources	Accorde l'autorisation de répertorier les ressources associées pour une liste de ressources issue d'une analyse des ressources. La réponse indique si chaque ressource renvoyée est déjà gérée par CloudFormation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceScanResources	Accorde l'autorisation de répertorier les ressources issues d'une analyse des ressources. Les résultats peuvent être filtrés par identifiant de ressource, préfixe de type de ressource, clé de balise et valeur de balise	List			
ListResourceScans	Accorde l'autorisation de répertorier les analyses de ressources du plus récent au plus ancien. Par défaut, il renverra jusqu'à 10 analyses de ressources	List			
ListStackInstanceResourceDrifts	Accorde l'autorisation de renvoyer des informations sur la dérive pour les ressources dont la dérive a été vérifiée dans l'instance de pile spécifiée	List	stackset*		
ListStackInstances	Accorde l'autorisation de renvoyer des informations récapitulatives sur les instances de piles associées à l'ensemble de piles spécifié	List	stackset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStackRefactorActions	Accorde l'autorisation de renvoyer la liste des actions du refactor de pile spécifié	List	stack*		
ListStackRefactors	Accorde l'autorisation de renvoyer l'ID et le statut de chaque refactor de pile actif	List	stack*		
ListStackResources	Accorde l'autorisation de renvoyer des descriptions de toutes les ressources de la pile spécifiée	List	stack*		
ListStackSetAutoDeploymentTargets	Accorde l'autorisation de renvoyer des informations récapitulatives sur les cibles de déploiement StackSet automatique	List	stackset*		
ListStackSetOperationResults	Accorde l'autorisation de renvoyer des informations récapitulatives sur les résultats d'une opération d'un ensemble de piles	Liste	stackset*		
ListStackSetOperations	Accorde l'autorisation de renvoyer des informations récapitulatives sur les opérations effectuées sur un ensemble de piles	Liste	stackset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStackSets	Accorde l'autorisation de renvoyer des informations récapitulatives sur les ensembles de piles associés à l'utilisateur	List			
ListStacks	Accorde l'autorisation de renvoyer les informations récapitulatives pour les piles dont le statut correspond à celui spécifié StackStatusFilter. En combinaison avec l' DescribeStacks action, accorde l'autorisation de répertorier les descriptions des piles	List			
ListTypeRegistrations	Accorde l'autorisation de répertorier CloudFormation les tentatives d'enregistrement	List			
ListTypeVersions	Accorde l'autorisation de répertorier les versions d'un CloudFormation type particulier	List			
ListTypes	Accorde l'autorisation de répertorier les CloudFormation types disponibles	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PublishType	Accorde l'autorisation de publier l'extension spécifiée dans le CloudFormation registre en tant qu'extension publique dans cette région	Écrire			
RecordHandlerProgress	Accorde l'autorisation d'enregistrer la progression du gestionnaire	Écrire	stack*		
RegisterPublisher	Accorde l'autorisation d'enregistrer un compte en tant qu'éditeur d'extensions publiques dans le CloudFormation registre	Écrire			
RegisterType	Autorise l'enregistrement d'un nouveau CloudFormation type	Écrire			
RollbackStack	Accorde l'autorisation de restaurer la pile au dernier état stable	Écrire	stack*		
				cloudformation:RoleArn	
SetStackPolicy	Accorde l'autorisation de définir une politique de pile d'une pile spécifiée	Gestion des autorisations	stack*		
				cloudformation:StackPolicyUrl	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetTypeConfiguration	Accorde l'autorisation de définir les données de configuration pour une CloudFormation extension enregistrée, dans le compte et la région donnés	Écrire			
SetTypeDefaultVersion	Accorde l'autorisation de définir quelle version d'un CloudFormation type s'applique aux CloudFormation opérations	Écrire			
SignalResource	Accorde l'autorisation d'envoyer un signal à la ressource spécifiée avec un état de succès ou d'échec	Écrire	stack*		
StartResourceScan	Autorise le lancement d'une analyse des ressources de ce compte dans cette région	Écrire			
StopStackSetOperation	Accorde l'autorisation d'arrêter une opération en cours sur un ensemble de piles et ses instances de piles associées	Écriture	stackset*		
TagResource	Accorde l'autorisation de baliser les ressources cloudformation	Identification	changeset		
			stack		
			stackset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} cloudformation:CreateAction	
TestType	Permet de tester une extension enregistrée afin de s'assurer qu'elle répond à toutes les exigences nécessaires pour être publiée dans le CloudFormation registre	Écrire			
UntagResource	Accorde l'autorisation de supprimer les balises des ressources cloudformation	Identification	changeset		
			stack		
			stackset		
				aws:TagKeys cloudformation:CreateAction	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGeneratedTemplate	Accorde l'autorisation de mettre à jour un modèle généré. Cela peut être utilisé pour modifier le nom, ajouter et supprimer des ressources, actualiser les ressources et modifier les UpdateReplacePolicy paramètres DeletionPolicy et	Écrire			
UpdateStack	Accorde l'autorisation de mettre à jour une pile comme spécifié dans le modèle	Écriture	stack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStackInstances	Accorde l'autorisation de mettre à jour les valeurs des paramètres pour les instances de piles pour les comptes spécifiés, dans les régions spécifiées	Écriture	stackset*		
			stackset-target		
			type		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				cloudformation:TargetRegion	
UpdateStackSet	Accorde l'autorisation de mettre à jour un jeu de pile comme spécifié dans le modèle	Écriture	stackset*		
			stackset-target		
			type		
				cloudformation:RoleArn cloudformation:TemplateUrl cloudformation:TargetRegion aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTerminationProtection	Accorde l'autorisation de mettre à jour la protection de terminaison pour la pile spécifiée	Écriture	stack*		
ValidateTemplate	Accorde l'autorisation de valider un modèle spécifié	Lecture		cloudformation:TemplateUrl	

Types de ressources définis par AWS CloudFormation

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
changeset	`arn:${Partition}:cloudformation:${Region}:${Account}:changeSet/${ChangeSetName}/${Id}`	aws:ResourceTag/${TagKey}
stack	`arn:${Partition}:cloudformation:${Region}:${Account}:stack/${StackName}/${Id}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
stackset	arn:${Partition}:cloudformation:${Region}:${Account}:stackset/${StackSetName}:${Id}	aws:ResourceTag/${TagKey}
stackset-target	arn:${Partition}:cloudformation:${Region}:${Account}:stackset-target/${StackSetTarget}	
type	arn:${Partition}:cloudformation:${Region}:${Account}:type/resource/${Type}	
typeHook	arn:${Partition}:cloudformation:${Region}:${Account}:type/hook/${Type}	
generated template	arn:${Partition}:cloudformation:${Region}:${Account}:generatedTemplate/${Id}	
resources can	arn:${Partition}:cloudformation:${Region}:${Account}:resourceScan/${Id}	

Clés de condition pour AWS CloudFormation

AWS CloudFormation définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
cloudformation:ChangeSetName	Filtre l'accès en fonction du nom du groupe de AWS CloudFormation modifications. Utilisez-le pour contrôler les jeux de modifications que les utilisateurs IAM peuvent exécuter ou supprimer	String
cloudformation:CreateAction	Filtre l'accès en fonction du nom d'une action d'API qui modifie les ressources. À utiliser pour contrôler quels utilisateurs APIs IAM peuvent utiliser pour ajouter ou supprimer des balises sur une pile ou un ensemble de piles	String
cloudformation:ImportResourceTypes	Filtre l'accès en fonction des types de ressources du modèle, tels que ::EC2 AWS : :Instance. Utilisez-le pour contrôler les types de ressources avec lesquels les utilisateurs IAM peuvent travailler lorsqu'ils souhaitent importer une ressource dans une pile	String
cloudformation:ResourceTypes	Filtre l'accès en fonction des types de ressources du modèle, tels que ::EC2 AWS : :Instance. Utilisez-les pour contrôler les types de ressource dont les utilisateurs IAM peuvent se servir lorsqu'ils créent ou mettent à jour une pile	ArrayOfString
cloudformation:RoleArn	Filtre l'accès en fonction de l'ARN d'un rôle de service IAM. Utilisez-le pour contrôler le rôle de service dont les	ARN

Clés de condition	Description	Type
	utilisateurs IAM peuvent se servir pour utiliser des piles ou des jeux de modifications	
cloudformation:StackPolicyUrl	Filtre l'accès en fonction d'une URL de politique de pile Amazon S3. Utilisez-la pour contrôler les politiques de pile que les utilisateurs IAM peuvent associer à une pile pendant la création ou la mise à jour de cette dernière.	String
cloudformation:TargetRegion	Filtre l'accès par région cible de jeu de piles. Utilisez-la pour contrôler les modèles auxquels les utilisateurs IAM peuvent se reporter lorsqu'ils créent ou mettent à jour des jeux de piles.	ArrayOfString
cloudformation:TemplateUrl	Filtre l'accès en fonction d'une URL de modèle Amazon S3. Utilisez-la pour contrôler les modèles auxquels les utilisateurs IAM peuvent se reporter lorsqu'ils créent ou mettent à jour des piles	String
cloudformation:TypeArn	Filtre l'accès par l'ARN d'une CloudFormation extension	ARN

Actions, ressources et clés de condition pour Amazon CloudFront

Amazon CloudFront (préfixe de service :`cloudfront`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudFront

- Types de ressources définis par Amazon CloudFront
- Clés de condition pour Amazon CloudFront

Actions définies par Amazon CloudFront

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison du journal automatique pour une distribution	Gestion des autorisations	distribution		
AssociateAlias	Accorde l'autorisation d'associer un alias à une CloudFront distribution	Écrire	distribution*		
AssociateDistributionTenantWebACL	Accorde l'autorisation d'associer un locataire de distribution à une AWS ACL Web WAF	Écrire	distribution-tenant*		
AssociateDistributionWebACL	Accorde l'autorisation d'associer une distribution à une AWS ACL Web WAF	Écrire	distribution*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CopyDistribution	Accorde l'autorisation de copier une distribution de distribution existante et de créer une distribution Web	Écrire	distribution*		cloudfront:CopyDistribution cloudfront:CreateDistribution cloudfront:GetDistribution
CreateAnycastIpList	Accorde l'autorisation de créer une liste d'adresses IP statique Anycast	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCachePolicy	Accorde l'autorisation d'ajouter une nouvelle politique de cache à CloudFront	Écrire			
CreateCloudFrontOriginAccessIdentity	Accorde l'autorisation de créer une nouvelle identité CloudFront d'accès à l'origine	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConnectionFunction	Accorde l'autorisation de créer une fonction de connexion	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectionGroup	Accorde l'autorisation de créer un groupe de connexion	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContinuousDeploymentPolicy	Accorde l'autorisation d'ajouter une nouvelle politique de déploiement continu à CloudFront	Écrire			
CreateDistribution	Accorde l'autorisation de créer une distribution Web	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	cloudfront:CreateConnectionGroup
CreateDistributionTenant	Autorise la création d'un locataire de distribution	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFieldLevelEncryptionConfig	Accorde l'autorisation de créer une configuration de chiffrement au niveau du champ	Écriture			
CreateFieldLevelEncryptionProfile	Accorde l'autorisation de créer un profil de chiffrement au niveau du champ	Écrire			
CreateFunction	Accorde l'autorisation de créer une CloudFront fonction	Écrire			
CreateInvalidation	Accorde l'autorisation de créer une nouvelle demande de lot d'invalidation	Écrire	distribution*		
CreateInvalidationForDistributionTenant	Accorde l'autorisation de créer une invalidation pour un locataire de distribution	Écrire	distribution-tenant*		
CreateKeyGroup	Accorde l'autorisation d'ajouter un nouveau groupe de clés à CloudFront	Écrire			
CreateKeyValueStore	Accorde l'autorisation de créer un CloudFront KeyValueStore	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMonitoringSubscription	Accorde l'autorisation d'activer des CloudWatch métriques supplémentaires pour la CloudFront distribution spécifiée. Les métriques supplémentaires entraînent un surcoût	Écrire			
CreateOriginAccessControl	Accorde l'autorisation de créer un nouveau contrôle d'accès d'origine	Écrire			
CreateOriginRequestPolicy	Accorde l'autorisation d'ajouter une nouvelle politique de demande d'origine à CloudFront	Écrire			
CreatePublicKey	Accorde l'autorisation d'ajouter une nouvelle clé publique à CloudFront	Écrire			
CreateRealtimeLogConfig	Accorde l'autorisation de créer une configuration de journalisation en temps réel	Écrire			
CreateResponseHeadersPolicy	Accorde l'autorisation d'ajouter une nouvelle politique d'en-têtes de réponse à CloudFront	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSavingsPlan [autorisation uniquement]	Accorde l'autorisation de créer un nouveau Savings Plan (plan d'épargne)	Écrire			
CreateStreamingDistribution	Accorde l'autorisation de créer une distribution RTMP	Écriture			
CreateStreamingDistributionWithTags	Accorde l'autorisation de créer une distribution RTMP avec des balises	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrustStore	Octroie l'autorisation de créer un magasin d'approbations.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcOrigin	Accorde l'autorisation de créer une origine VPC	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnycastIpList	Accorde l'autorisation de supprimer une liste d'adresses IP statiques Anycast	Écrire	anycast-ip-list*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCachePolicy	Accorde l'autorisation de supprimer une politique de cache	Écrire	cache-policy*		
DeleteCloudFrontOriginAccessIdentity	Accorde l'autorisation de supprimer une identité CloudFront d'accès d'origine	Écrire	origin-access-identity*		
DeleteConnectionFunction	Autorise la suppression d'une fonction de connexion	Écrire	connection-function*		
DeleteConnectionGroup	Accorde l'autorisation de supprimer un groupe de connexion	Écrire	connection-group*		
DeleteContinuousDeploymentPolicy	Accorde l'autorisation de supprimer une politique de déploiement continu	Écrire	continuous-deployment-policy*		
DeleteDistribution	Accorde l'autorisation de supprimer une distribution Web	Écrire	distribution*		
DeleteDistributionTenant	Autorise la suppression d'un locataire de distribution	Écrire	distribution-tenant*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFieldLevelEncryptionConfig	Accorde l'autorisation de supprimer une configuration de chiffrement au niveau du champ	Écriture	field-level-encryption-config*		
DeleteFieldLevelEncryptionProfile	Accorde l'autorisation de supprimer un profil de chiffrement au niveau du champ	Écrire	field-level-encryption-profile*		
DeleteFunction	Autorise la suppression d'une CloudFront fonction	Écrire	function*		
DeleteKeyGroup	Accorde l'autorisation de supprimer un groupe de clés	Écrire			
DeleteKeyValueStore	Accorde l'autorisation de supprimer un CloudFront KeyValueStore	Écrire	key-value-store*		
DeleteMonitoringSubscription	Accorde l'autorisation de désactiver des CloudWatch métriques supplémentaires pour la CloudFront distribution spécifiée	Écrire			
DeleteOriginAccessControl	Accorde l'autorisation de supprimer un contrôle d'accès d’origine	Écrire	origin-access-control*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteOriginRequestPolicy	Accorde l'autorisation de supprimer une politique de demande d'origine	Écrire	origin-request-policy*		
DeletePublicKey	Accorde l'autorisation de supprimer une clé publique de CloudFront	Écrire			
DeleteRealtimeLogConfig	Accorde l'autorisation de supprimer une configuration de journalisation en temps réel	Écrire	realtime-log-config*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer le document de politique d'une ressource	Écrire	vpcorigin		
DeleteResponseHeadersPolicy	Accorde l'autorisation de supprimer une politique d'en-têtes de réponses	Écrire	response-headers-policy*		
DeleteStreamingDistribution	Accorde l'autorisation de supprimer une distribution RTMP	Écrire	streaming-distribution*		
DeleteTrustStore	Autorise la suppression d'un trust store	Écrire	trust-store*		
DeleteVpcOrigin	Accorde l'autorisation de supprimer une origine VPC	Écrire	vpcorigin*		
DescribeConnectionFunction	Accorde l'autorisation d'obtenir un résumé de la fonction de connexion	Lecture	connection-function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFunction	Accorde l'autorisation d'obtenir un résumé des CloudFront fonctions	Lecture	function*		
DescribeKeyValueStore	Accorde l'autorisation d'obtenir un CloudFront KeyValueStore résumé	Lecture	key-value-store*		
DisassociateDistributionTenantWebACL	Accorde l'autorisation de dissocier un locataire de distribution d'une ACL AWS Web WAF	Écrire	distribution-tenant*		
DisassociateDistributionWebACL	Accorde l'autorisation de dissocier une distribution d'une ACL AWS Web WAF	Écrire	distribution*		
GetAnycastIpList	Accorde l'autorisation d'obtenir une liste d'adresses IP statiques Anycast	Lecture	anycast-ip-list*		
GetCachePolicy	Accorde l'autorisation d'obtenir la politique de cache	Lecture	cache-policy*		
GetCachePolicyConfig	Accorde l'autorisation d'obtenir la configuration de la politique de cache	Lecture	cache-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCloudFrontOriginAccessIdentity	Accorde l'autorisation d'obtenir les informations relatives à une identité CloudFront d'accès d'origine	Lecture	origin-access-identity*		
GetCloudFrontOriginAccessIdentityConfig	Accorde l'autorisation d'obtenir les informations de configuration relatives à une identité d'accès à l'origine Cloudfront	Lecture	origin-access-identity*		
GetConnectionFunction	Accorde l'autorisation d'obtenir le code d'une fonction de connexion	Lecture	connection-function*		
GetConnectionGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de connexion	Lecture	connection-group*		
GetConnectionGroupByRoutingEndpoint	Accorde l'autorisation d'obtenir des informations sur un groupe de connexion par le point de terminaison de routage spécifié	Lecture	connection-group*		
GetContinuousDeploymentPolicy	Accorde l'autorisation d'obtenir la configuration de la politique de cache	Lecture	continuous-deployment-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContinuousDeploymentPolicyConfig	Accorde l'autorisation d'obtenir la configuration de la politique de déploiement continu	Lecture	continuous-deployment-policy*		
GetDistribution	Accorde l'autorisation d'obtenir les informations sur une distribution Web	Lecture	distribution*		
GetDistributionConfig	Accorde l'autorisation d'obtenir des informations sur la configuration d'une distribution	Lecture	distribution*		
GetDistributionTenant	Accorde l'autorisation d'obtenir des informations sur un locataire de distribution	Lecture	distribution-tenant*		
GetDistributionTenantByDomain	Accorde l'autorisation d'obtenir des informations sur un locataire de distribution par le domaine associé	Lecture	distribution-tenant*		
GetFieldLevelEncryption	Accorde l'autorisation d'obtenir les informations de configuration de chiffrement au niveau du champ	Lecture	field-level-encryption-config*		
GetFieldLevelEncryptionConfig	Accorde l'autorisation d'obtenir les informations de configuration de chiffrement au niveau du champ	Lecture	field-level-encryption-config*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFieldLevelEncryptionProfile	Accorde l'autorisation d'obtenir les informations de configuration de chiffrement au niveau du champ	Lecture	field-level-encryption-profile*		
GetFieldLevelEncryptionProfileConfig	Accorde l'autorisation d'obtenir les informations de configuration du profil de chiffrement au niveau du champ	Lecture	field-level-encryption-profile*		
GetFunction	Accorde l'autorisation d'obtenir le code d'une CloudFront fonction	Lecture	function*		
GetInvalidation	Accorde l'autorisation d'obtenir les informations relatives à une invalidation	Lecture	distribution*		
GetInvalidationForDistributionTenant	Accorde l'autorisation d'obtenir des informations sur une invalidation pour un locataire de distribution	Lecture	distribution-tenant*		
GetKeyGroup	Accorde l'autorisation d'obtenir un groupe de clés	Lecture			
GetKeyGroupConfig	Accorde l'autorisation d'obtenir une configuration de groupe de clés	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetManagedCertificateDetails	Accorde l'autorisation d'obtenir des informations sur un certificat CloudFront géré	Lecture	distribution-tenant*		
GetMonitoringSubscription	Accorde l'autorisation d'obtenir des informations indiquant si CloudWatch des métriques supplémentaires sont activées pour la CloudFront distribution spécifiée	Lecture			
GetOriginAccessControl	Accorde l'autorisation d'obtenir un contrôle d'accès d'origine	Lecture	origin-access-control*		
GetOriginAccessControlConfig	Accorde l'autorisation d'obtenir la configuration de contrôle d'accès d'origine	Lecture	origin-access-control*		
GetOriginRequestPolicy	Accorde l'autorisation d'obtenir la politique de demande d'origine	Lecture	origin-request-policy*		
GetOriginRequestPolicyConfig	Accorde l'autorisation d'obtenir la configuration de la politique de demande d'origine	Lecture	origin-request-policy*		
GetPublicKey	Accorde l'autorisation d'obtenir les informations sur la clé publique	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPublicKeyConfig	Accorde l'autorisation d'obtenir des informations sur la configuration de la clé publique	Lecture			
GetRealtimeLogConfig	Accorde l'autorisation d'obtenir une configuration de journal en temps réel	Lecture	realtime-log-config*		
GetResourcePolicy	Accorde l'autorisation d'obtenir des informations sur le document de politique d'une ressource	Lecture	vpcorigin		
GetResponseHeadersPolicy	Accorde l'autorisation d'obtenir la politique d'en-têtes de réponses	Lecture	response-headers-policy*		
GetResponseHeadersPolicyConfig	Accorde l'autorisation d'obtenir la configuration de la politique d'en-têtes de réponses	Lecture	response-headers-policy*		
GetSavingsPlan [autorisation uniquement]	Accorde l'autorisation d'obtenir un Savings Plan (plan d'épargne)	Lecture			
GetStreamingDistribution	Accorde l'autorisation d'obtenir les informations sur une distribution RTMP	Lecture	streaming-distribution*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStreamingDistributionConfig	Accorde l'autorisation d'obtenir les informations de configuration d'une distribution de streaming	Lecture	streaming-distribution*		
GetTrustStore	Accorde l'autorisation d'obtenir des informations sur un trust store	Lecture	trust-store*		
GetVpcOrigin	Accorde l'autorisation d'obtenir les informations relatives à l'origine d'un VPC	Lecture	vpcorigin*		
ListAnycastIpLists	Accorde l'autorisation de répertorier vos listes d'adresses IP statiques Anycast	List			
ListCachePolicies	Accorde l'autorisation de répertorier toutes les politiques de cache créées CloudFront pour ce compte	List			
ListCloudFrontOriginAccessIdentities	Accorde l'autorisation de répertorier vos identités CloudFront d'accès d'origine	List			
ListConflictingAliases	Accorde l'autorisation de répertorier tous les alias en conflit avec l'alias donné dans CloudFront	List	distribution*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConnectionFunctions	Accorde l'autorisation de répertorier les fonctions de connexion dans votre Compte AWS	List			
ListConnectionGroups	Accorde l'autorisation de répertorier les groupes de connexion dans votre Compte AWS	List			
ListContinuousDeploymentPolicies	Accorde l'autorisation de répertorier toutes les politiques de déploiement continu dans le compte	List			
ListDistributionTenants	Accorde l'autorisation de répertorier les locataires de distribution dans votre Compte AWS	List			
ListDistributionTenantsByCustomization	Accorde l'autorisation de répertorier les locataires de distribution selon la personnalisation que vous spécifiez	List			
ListDistributions	Accorde l'autorisation de répertorier les distributions associées à votre Compte AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDistributionsByAnycastIpListId	Accorde l'autorisation de répertorier les distributions de votre compte associées à la valeur spécifiée AnycastIp ListId	List			
ListDistributionsByCachePolicyId	Accorde l'autorisation de répertorier la distribution IDs pour les distributions dont le comportement de cache est associé à la politique de cache spécifiée	List			
ListDistributionsByConnectionFunction	Accorde l'autorisation de répertorier les résumés des distributions associées à la fonction de connexion spécifiée	List	connection-function*		
ListDistributionsByConnectionMode	Accorde l'autorisation de répertorier les distributions selon le mode de connexion spécifié	List			
ListDistributionsByKeyGroup	Accorde l'autorisation de répertorier la distribution IDs pour les distributions dont le comportement de cache est associé au groupe de clés spécifié	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDistributionsByLambdaFunction [autorisation uniquement]	Accorde l'autorisation de répertorier les distributions associées à une fonction Lambda	List			
ListDistributionsByOriginRequestPolicyId	Accorde l'autorisation de répertorier la distribution IDs pour les distributions dont le comportement de cache est associé à la politique de demande d'origine spécifiée	List			
ListDistributionsByRealtimeLogConfig	Accorde l'autorisation d'obtenir une liste de distributions dont le comportement de cache est associé à la configuration de journal en temps réel spécifiée	List			
ListDistributionsByResponseHeadersPolicyId	Accorde l'autorisation de répertorier la distribution IDs pour les distributions dont le comportement de cache est associé à la politique d'en-têtes de réponse spécifiée	List			
ListDistributionsByTrustStore	Accorde l'autorisation de répertorier les résumés des distributions associées au trust store spécifié	List	trust-store*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDistributionsByVpcOriginId	Accorde l'autorisation de répertorier IDs les distributions associées à l'origine VPC spécifiée	List			
ListDistributionsByWebACLId	Accorde l'autorisation de répertorier les distributions associées à votre Compte AWS ACL Web AWS WAF donné	List			
ListDomainConflicts	Accorde l'autorisation de répertorier les conflits de domaine pour un domaine spécifié	List	distribution distribution-tenant		
ListFieldLevelEncryptionConfigs	Accorde l'autorisation de répertorier toutes les configurations de chiffrement au niveau des champs qui ont été créées CloudFront pour ce compte	List			
ListFieldLevelEncryptionProfiles	Accorde l'autorisation de répertorier tous les profils de chiffrement au niveau des champs qui ont été créés CloudFront pour ce compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFunctions	Accorde l'autorisation d'obtenir une liste de CloudFront fonctions	List			
ListInvalidations	Accorde l'autorisation de répertorier vos lots d'invalidation	List	distribution*		
ListInvalidationsForDistributionTenant	Accorde l'autorisation de répertorier les invalidations pour un locataire de distribution	List	distribution-tenant*		
ListKeyGroups	Accorde l'autorisation de répertorier tous les groupes clés créés CloudFront pour ce compte	List			
ListKeyValueStores	Accorde l'autorisation d'obtenir une liste de CloudFront KeyValueStores	List			
ListOriginAccessControls	Accorde l'autorisation de répertorier tous les contrôles d'accès d'origine dans le compte	List			
ListOriginRequestPolicies	Accorde l'autorisation de répertorier toutes les politiques de demande d'origine créées CloudFront pour ce compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPublicKeys	Accorde l'autorisation de répertorier toutes les clés publiques ajoutées CloudFront à ce compte	List			
ListRateCards [autorisation uniquement]	Accorde l'autorisation de répertorier les cartes CloudFront tarifaires pour le compte	List			
ListRealtimeLogConfigs	Accorde l'autorisation d'obtenir une liste de configurations de journal en temps réel	List			
ListResponseHeadersPolicies	Accorde l'autorisation de répertorier toutes les politiques d'en-têtes de réponse créées CloudFront pour ce compte	List			
ListSavingsPlans [autorisation uniquement]	Accorde l'autorisation de répertorier les Savings Plans (plans d'épargne) dans le compte	List			
ListStreamingDistributions	Accorde l'autorisation de répertorier vos distributions RTMP	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une CloudFront ressource	Lecture	anycast-ip-list		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			connection-function		
			connection-group		
			distribution		
			distribution-tenant		
			trust-store		
			vpcorigin		
ListTrustStores	Accorde l'autorisation de répertorier les magasins de confiance de votre Compte AWS	List			
ListUsages [autorisation uniquement]	Autorise l' CloudFront utilisation des listes	List			
ListVpcOrigins	Accorde l'autorisation de répertorier les origines des VPC	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PublishConnectionFunction	Accorde l'autorisation de publier une fonction de connexion	Écrire	connection-function*		
PublishFunction	Autorise la publication d'une CloudFront fonction	Écrire	function*		
PutResourcePolicy	Accorde l'autorisation de mettre à jour ou de créer le document de politique d'une ressource	Écrire	vpcorigin		
TagResource	Accorde l'autorisation d'ajouter des balises à une CloudFront ressource	Identification	anycast-ip-list		
			connection-function		
			connection-group		
			distribution		
			distribution-tenant		
			streaming-distribution		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			trust-store		
			vpcorigin		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestConnectionFunction	Accorde l'autorisation de tester une fonction de connexion	Écrire	connection-function*		
TestFunction	Accorde l'autorisation de tester une CloudFront fonction	Écrire	function*		
UntagResource	Accorde l'autorisation de supprimer des balises d'une CloudFront ressource	Identification	anycast-ip-list		
			connection-function		
			connection-group		
			distribution		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			distribution-tenant		
			streaming-distribution		
			trust-store		
			vpcorigin		
				aws:TagKeys	
UpdateAnycastIpList	Autorise la mise à jour d'une liste d'adresses IP statiques Anycast	Écrire	anycast-ip-list*		
UpdateCachePolicy	Accorde l'autorisation de mettre à jour une politique de cache	Écrire	cache-policy*		
UpdateCloudFrontOriginAccessIdentity	Accorde l'autorisation de définir la configuration d'une identité CloudFront d'accès d'origine	Écrire	origin-access-identity*		
UpdateConnectionFunction	Autorise la mise à jour d'une fonction de connexion	Écrire	connection-function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConnectionGroup	Accorde l'autorisation de mettre à jour un groupe de connexion	Écrire	connection-group*		
UpdateContinuousDeploymentPolicy	Accorde l'autorisation de mettre à jour une politique de déploiement continu	Écrire	continuous-deployment-policy*		
UpdateDistribution	Accorde l'autorisation de mettre à jour une configuration de distribution Web	Écrire	distribution*		
UpdateDistributionTenant	Autorise la mise à jour d'un tenant de distribution	Écrire	distribution-tenant*		
UpdateDistributionWithStagingConfig	Accorde l'autorisation de copier la configuration d'une distribution Web intermédiaire vers la distribution Web principale correspondante	Écrire	distribution*		
UpdateDomainAssociation	Autorise la mise à jour d'une association de domaines	Écrire	distribution		
			distribution-tenant		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFieldLevelEncryptionConfig	Accorde l'autorisation de mettre à jour la configuration de chiffrement au niveau du champ	Écriture			
UpdateFieldLevelEncryptionProfile	Accorde l'autorisation de mettre à jour un profil de chiffrement au niveau du champ	Écrire	field-level-encryption-profile*		
UpdateFunction	Autorise la mise à jour d'une CloudFront fonction	Écrire	function*		
UpdateKeyGroup	Accorde l'autorisation de mettre à jour un groupe de clés	Écrire			
UpdateKeyValueStore	Accorde l'autorisation de mettre à jour un CloudFront KeyValueStore	Écrire	key-value-store*		
UpdateOriginAccessControl	Accorde l'autorisation de mettre à jour un contrôle d'accès d'origine	Écrire	origin-access-control*		
UpdateOriginRequestPolicy	Accorde l'autorisation de mettre à jour une politique de demande d'origine	Écriture	origin-request-policy*		
UpdatePublicKey	Accorde l'autorisation de mettre à jour les informations de clé publique	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRealtimeLogConfig	Accorde l'autorisation de mettre à jour une configuration de journal en temps réel	Écrire	realtime-log-config*		
UpdateResponseHeadersPolicy	Accorde l'autorisation de mettre à jour une politique d'en-têtes de réponses	Écrire	response-headers-policy*		
UpdateSavingsPlan [autorisation uniquement]	Accorde l'autorisation de mettre à jour un savings plan (plan d'épargne)	Écrire			
UpdateStreamingDistribution	Accorde l'autorisation de mettre à jour une configuration de distribution RTMP	Écrire	streaming-distribution*		
UpdateTrustStore	Autorise la mise à jour d'un trust store	Écrire	trust-store*		
UpdateVpcOrigin	Accorde l'autorisation de mettre à jour l'origine d'un VPC	Écrire	vpcorigin*		
VerifyDnsConfiguration	Accorde l'autorisation de vérifier la configuration DNS pour un domaine spécifié	Lecture	distribution-tenant		

Types de ressources définis par Amazon CloudFront

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
distribution	`arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}`	aws:ResourceTag/${TagKey}
streaming-distribution	`arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}`	aws:ResourceTag/${TagKey}
origin-access-identity	`arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}`	
field-level-encryption-config	`arn:${Partition}:cloudfront::${Account}:field-level-encryption-config/${Id}`	
field-level-encryption-profile	`arn:${Partition}:cloudfront::${Account}:field-level-encryption-profile/${Id}`	
cache-policy	`arn:${Partition}:cloudfront::${Account}:cache-policy/${Id}`	
origin-request-policy	`arn:${Partition}:cloudfront::${Account}:origin-request-policy/${Id}`	
realtime-log-config	`arn:${Partition}:cloudfront::${Account}:realtime-log-config/${Name}`	
function	`arn:${Partition}:cloudfront::${Account}:function/${Name}`	

Types de ressources	ARN	Clés de condition
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${Name}	
response-headers-policy	arn:${Partition}:cloudfront::${Account}:response-headers-policy/${Id}	
origin-access-control	arn:${Partition}:cloudfront::${Account}:origin-access-control/${Id}	
continuous-deployment-policy	arn:${Partition}:cloudfront::${Account}:continuous-deployment-policy/${Id}	
anycast-ip-list	arn:${Partition}:cloudfront::${Account}:anycast-ip-list/${Id}	aws:ResourceTag/${TagKey}
vpcorigin	arn:${Partition}:cloudfront::${Account}:vpcorigin/${Id}	aws:ResourceTag/${TagKey}
distribution-tenant	arn:${Partition}:cloudfront::${Account}:distribution-tenant/${Id}	aws:ResourceTag/${TagKey}
connection-group	arn:${Partition}:cloudfront::${Account}:connection-group/${Id}	aws:ResourceTag/${TagKey}
trust-store	arn:${Partition}:cloudfront::${Account}:trust-store/${Id}	aws:ResourceTag/${TagKey}
connection-function	arn:${Partition}:cloudfront::${Account}:connection-function/${Id}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudFront

Amazon CloudFront définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudFront KeyValueStore

Amazon CloudFront KeyValueStore (préfixe de service :`cloudfront-keyvaluestore`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudFront KeyValueStore
- Types de ressources définis par Amazon CloudFront KeyValueStore
- Clés de condition pour Amazon CloudFront KeyValueStore

Actions définies par Amazon CloudFront KeyValueStore

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteKey	Octroie l'autorisation de supprimer la paire clé-valeur spécifiée par la clé.	Écrire	key-value-store*		
DescribeKeyValueStore	Octroie l'autorisation de renvoyer des informations de métadonnées sur KeyValueStore.	Lecture	key-value-store*		
GetKey	Octroie l'autorisation de renvoyer une paire clé-valeur.	Lecture	key-value-store*		
ListKeys	Octroie l'autorisation de renvoyer une liste de paires clé-valeur.	List	key-value-store*		
PutKey	Octroie l'autorisation de créer une nouvelle paire clé-valeur ou de remplacer la valeur d'une clé existante.	Écrire	key-value-store*		
UpdateKeys	Accorde l'autorisation de mettre ou de supprimer plusieurs paires clé-valeur	Écrire	key-value-store*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	en une seule all-or-nothing opération				

Types de ressources définis par Amazon CloudFront KeyValueStore

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
key-value-store	`arn:${Partition}:cloudfront::${Account}:key-value-store/${ResourceId}`	

Clés de condition pour Amazon CloudFront KeyValueStore

CloudFront KeyValueStore ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS CloudHSM

AWS CloudHSM (préfixe de service `cloudhsm` :) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CloudHSM
- Types de ressources définis par AWS CloudHSM
- Clés de condition pour AWS CloudHSM

Actions définies par AWS CloudHSM

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CopyBackupToRegion	Accorde l'autorisation de créer une copie d'une sauvegarde dans la région spécifiée	Écrire	backup*		cloudhsm:CopyBackupToRegion cloudhsm:TagResource cloudhsm:UntagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCluster	Accorde l'autorisation de créer un nouveau cluster AWS CloudHSM	Écrire	backup		cloudhsm:TagResource ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:RevokeSecurityGroupEgress iam:CreateServiceL

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					inkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateHsm	Accorde l'autorisation de créer un nouveau module de sécurité matériel (HSM) dans le cluster CloudHSM spécifié AWS	Écrire	cluster*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeSubnets ec2:RevokeSecurityGroupEgress
DeleteBackup	Accorde l'autorisation de supprimer la sauvegarde CloudHSM spécifiée	Écrire	backup*		
DeleteCluster	Accorde l'autorisation de supprimer le cluster AWS CloudHSM spécifié	Écrire	cluster*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup
DeleteHsm	Accorde l'autorisation de supprimer le module HSM spécifié	Écrire			ec2:DeleteNetworkInterface
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique attachée aux ressources CloudHSM	Écrire	backup*		
DescribeBackups	Accorde l'autorisation d'obtenir des informations sur les sauvegardes des clusters AWS CloudHSM	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeClusters	Accorde l'autorisation d'obtenir des informations sur les clusters AWS CloudHSM	Lecture			
GetResourcePolicy	Accorde l'autorisation d'obtenir des informations sur la politique attachée à une ressource AWS CloudHSM	Lecture	backup*		
InitializeCluster	Accorde l'autorisation de revendiquer un cluster AWS CloudHSM	Écrire	cluster*		
ListTags	Accorde l'autorisation d'obtenir une liste de balises pour le cluster AWS CloudHSM spécifié	Lecture	backup		
			cluster		
ModifyBackupAttributes	Accorde l'autorisation de modifier les attributs d'une sauvegarde AWS CloudHSM	Écrire	backup*		
ModifyCluster	Accorde l'autorisation de modifier le cluster AWS CloudHSM	Écrire	cluster*		ec2:DescribeSubnets
PutResourcePolicy	Accorde l'autorisation d'associer une politique à une ressource AWS CloudHSM	Écrire	backup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreBackup	Accorde l'autorisation de restaurer la sauvegarde CloudHSM spécifiée	Écrire	backup*		
TagResource	Accorde l'autorisation d'ajouter ou de remplacer une ou plusieurs balises pour le cluster CloudHSM spécifié AWS	Identification	backup		
			cluster		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer la ou les balises spécifiées du cluster AWS CloudHSM spécifié	Identification	backup		
			cluster		
				aws:TagKeys	

Types de ressources définis par AWS CloudHSM

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
backup	`arn:${Partition}:cloudhsm:${Region}:${Account}:backup/${CloudHsmBackupInstanceName}`	aws:ResourceTag/${TagKey}
cluster	`arn:${Partition}:cloudhsm:${Region}:${Account}:cluster/${CloudHsmClusterInstanceName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS CloudHSM

AWS CloudHSM définit les clés de condition suivantes qui peuvent être utilisées dans `Condition` l'élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudSearch

Amazon CloudSearch (préfixe de service :`cloudsearch`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudSearch
- Types de ressources définis par Amazon CloudSearch
- Clés de condition pour Amazon CloudSearch

Actions définies par Amazon CloudSearch

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTags	Attache des balises de ressources à un CloudSearch domaine Amazon	Identification	domain*		
BuildSuggesters	Indexe les suggestions de recherche	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDomain	Crée un nouveau domaine de recherche	Écrire	domain*		
DefineAnalysisScheme	Configure une méthode d'analyse pouvant être appliquée à un champ de texte ou de tableau de texte pour définir des options de traitement de texte propres à une langue	Écrire	domain*		
DefineExpression	Configure un élément Expression pour le domaine de recherche	Écrire	domain*		
DefineIndexField	Configure et IndexField pour le domaine de recherche	Écrire	domain*		
DefineSuggester	Configure un outil de suggestion pour un domaine	Écrire	domain*		
DeleteAnalysisScheme	Supprime une méthode d'analyse	Écrire	domain*		
DeleteDomain	Supprime définitivement un domaine de recherche et toutes ses données	Écrire	domain*		
DeleteExpression	Supprime un élément Expression du domaine de recherche	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteIndexField	Supprime un IndexField du domaine de recherche	Écrire	domain*		
DeleteSuggester	Supprime un outil de suggestion	Écrire	domain*		
DescribeAnalysisSchemes	Récupère les méthodes d'analyse configurées pour un domaine	Lecture	domain*		
DescribeAvailabilityOptions	Récupère les options de disponibilité configurées pour un domaine	Lecture	domain*		
DescribeDomainEndpointOptions	Récupère les options de point de terminaison de domaine configurées pour un domaine	Lecture	domain*		
DescribeDomains	Récupère des informations sur les domaines de recherche appartenant à ce compte	List	domain*		
DescribeExpressions	Récupère les expressions configurées pour le domaine de recherche	Lecture	domain*		
DescribeIndexFields	Récupère des informations sur les champs d'index configurés pour le domaine de recherche	Lecture	domain*		
DescribeScalingParameters	Récupère les paramètres de mise à l'échelle configurés pour un domaine	Lecture	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeServiceAccessPolicies	Récupère des informations sur les stratégies d'accès qui contrôlent l'accès aux points de terminaison de document et de recherche du domaine	Lecture	domain*		
DescribeSuggesters	Récupère les outils de suggestion configurés pour un domaine	Lecture	domain*		
IndexDocuments	Indique au domaine de recherche qu'il doit démarrer l'indexation de ses documents en utilisant les dernières options d'indexation	Écrire	domain*		
ListDomainNames	Répertorie tous les domaines de recherche appartenant à un compte	List	domain*		
ListTags	Affiche toutes les balises de ressources pour un CloudSearch domaine Amazon	Lecture	domain*		
RemoveTags	Supprime les balises de ressource spécifiées d'un domaine Amazon ES	Identification	domain*		
UpdateAvailabilityOptions	Configure les options de disponibilité d'un domaine	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDomainEndpointOptions	Configure les options de point de terminaison de domaine pour un domaine	Écrire	domain*		
UpdateScalingParameters	Configure les paramètres de mise à l'échelle d'un domaine	Écrire	domain*		
UpdateServiceAccessPolicies	Configure les règles d'accès qui contrôlent l'accès aux points de terminaison de document et de recherche du domaine	Gestion des autorisations	domain*		
document [autorisation uniquement]	Autorise l'accès aux opérations de service de document	Écrire	domain		
search [autorisation uniquement]	Autorise l'accès aux opérations de recherche	Lecture	domain		
suggest [autorisation uniquement]	Autorise l'accès aux opérations de suggestion	Lecture	domain		

Types de ressources définis par Amazon CloudSearch

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> Pour plus d'informations sur l'utilisation CloudSearch des ressources Amazon ARNs dans le cadre d'une politique IAM, consultez Amazon CloudSearch ARNs dans le manuel Amazon CloudSearch Developer Guide.

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:cloudsearch:${Region}:${Account}:domain/${DomainName}`	

Clés de condition pour Amazon CloudSearch

CloudSearch ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS CloudShell

AWS CloudShell (préfixe de service :`cloudshell`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CloudShell
- Types de ressources définis par AWS CloudShell

- Clés de condition pour AWS CloudShell

Actions définies par AWS CloudShell

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApproveCommand [autorisation uniquement]	Accorde l'autorisation d'approuver une commande envoyée par un autre AWS service	Lecture	Environment*		
CreateEnvironment [autorisation uniquement]	Accorde les autorisations nécessaires à la création d'un CloudShell environnement	Écrire		cloudshell:SecurityGroupIds cloudshell:SubnetIds cloudshell:VpcIds	
CreateSession [autorisation uniquement]	Accorde l'autorisation de se connecter à un CloudShell environnement depuis le AWS Management Console	Écrire	Environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEnvironment [autorisation uniquement]	Accorde l'autorisation de supprimer un CloudShell environnement	Écrire	Environment*		
DescribeEnvironments [autorisation uniquement]	Accorde l'autorisation de renvoyer des descriptions des environnements utilisateur existants	List			
GetEnvironmentStatus [autorisation uniquement]	Autorise la lecture de CloudShell l'état d'un environnement	Lecture	Environment*		
GetFileDownloadUrls [autorisation uniquement]	Accorde l'autorisation de télécharger des fichiers depuis un CloudShell environnement	Écrire	Environment*		
GetFileUploadUrls [autorisation uniquement]	Accorde des autorisations pour télécharger des fichiers dans un CloudShell environnement	Écrire	Environment*		
PutCredentials [autorisation uniquement]	Accorde les autorisations de transférer les informations d'identification de la console vers l'environnement	Écriture	Environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartEnvironment [autorisation uniquement]	Accorde l'autorisation de démarrer un CloudShell environnement arrêté	Écrire	Environment*		
StopEnvironment [autorisation uniquement]	Autorise l'arrêt d'un CloudShell environnement en cours d'exécution	Écrire	Environment*		

Types de ressources définis par AWS CloudShell

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Environment	`arn:${Partition}:cloudshell:${Region}:${Account}:environment/${EnvironmentId}`	

Clés de condition pour AWS CloudShell

AWS CloudShell définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
cloudshell:SecurityGroupIds	Filtre l'accès par identifiant de groupe de sécurité. Disponible pendant le CreateEnvironment fonctionnement	ArrayOfString
cloudshell:SubnetIds	Filtre l'accès par identifiant de sous-réseau. Disponible pendant le CreateEnvironment fonctionnement	ArrayOfString
cloudshell:VpcIds	Filtre l'accès par identifiants VPC. Disponible pendant le CreateEnvironment fonctionnement	ArrayOfString

Actions, ressources et clés de condition pour AWS CloudTrail

AWS CloudTrail (préfixe de service :`cloudtrail`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CloudTrail
- Types de ressources définis par AWS CloudTrail
- Clés de condition pour AWS CloudTrail

Actions définies par AWS CloudTrail

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTags	Autorise l'ajout d'une ou plusieurs balises à un parcours, à une banque de données d'événements, à une chaîne ou à un tableau de bord, dans la limite de 50	Identification	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelQuery	Accorde l'autorisation d'annuler une requête en cours d'exécution	Écrire	eventdatastore*		
CreateChannel	Accorde l'autorisation de créer un canal.	Écrire	channel*		cloudtrail:AddTags
			eventdatastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Accorde l'autorisation de créer un tableau de bord	Écrire	dashboard*		cloudtrail:AddTags cloudtrail:StartDashboardRefresh cloudtrail:StartQuery
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEventDataStore	Accorde l'autorisation de créer un magasin de données d'événement	Écrire	eventdatastore*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateServiceLinkedChannel [autorisation uniquement]	Accorde l'autorisation de créer un canal lié à un service qui spécifie les paramètres de livraison des données de journal à un service AWS	Écrire	channel*		
CreateTrail	Accorde l'autorisation de créer un journal d'activité qui spécifie les paramètres pour la livraison de données de journal dans un compartiment Amazon S3.	Écrire	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Accorde l'autorisation de supprimer un canal.	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDashboard	Accorde l'autorisation de supprimer un tableau de bord	Écrire	dashboard*		
DeleteEventDataStore	Accorde l'autorisation de supprimer un magasin de données d'événement	Écrire	eventdatastore*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource d'un plan de réponse.	Écrire	channel		
			dashboard		
			eventdatastore		
DeleteServiceLinkedChannel [autorisation uniquement]	Accorde l'autorisation de supprimer un canal lié à un service	Écrire	channel*		
DeleteTrail	Accorde l'autorisation de supprimer un journal d'activité.	Écrire	trail*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterOrganizationDelegatedAdmin	Accorde l'autorisation de désenregistrer le compte d'un membre AWS d'Organizations en tant qu'administrateur délégué	Écrire			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization
DescribeQuery	Accorde l'autorisation de répertorier les détails de la requête	Lecture	eventdatastore*		
DescribeTrails	Accorde l'autorisation de répertorier les paramètres des journaux d'activité associés à la région actuelle de votre compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableFederation	Accorde l'autorisation de désactiver la fédération des données du magasin de données d'événements à l'aide du catalogue de données AWS Glue	Écrire	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableFederation	Accorde l'autorisation d'activer la fédération des données du magasin de données événementielles à l'aide du catalogue de données AWS Glue	Écrire	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GenerateQuery	Accorde l'autorisation de générer une requête pour un magasin de données d'événements spécifié à l'aide du générateur de requêtes CloudTrail Lake	Écrire	eventdatastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GenerateQueryResultsSummary [autorisation uniquement]	Accorde l'autorisation de générer un résumé des résultats pour des requêtes spécifiées à l'aide du générateur de langage CloudTrail naturel	Lecture	eventdatastore*		cloudtrail:GetQueryResults kms:Decrypt kms:GenerateDataKey
GetChannel	Accorde l'autorisation de renvoyer les informations à propos d'une chaîne spécifique	Lecture	channel*		
GetDashboard	Accorde l'autorisation de répertorier les paramètres du tableau de bord	Lecture	dashboard*		
GetEventConfiguration	Accorde l'autorisation de répertorier les configurations d'événements configurées pour un journal ou un magasin de données d'événements	Lecture	eventdatastore		
			trail		
GetEventDataStore	Accorde l'autorisation de répertorier les paramètres du magasin de données d'événement	Lecture	eventdatastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEventDataStoreData	Accorde l'autorisation d'obtenir des données d'un magasin de données d'événements à l'aide du catalogue de données AWS Glue	Lecture	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetEventSelectors	Accorde l'autorisation de répertorier les paramètres des sélecteurs d'événements configurés pour un journal d'activité	Lecture	trail*		
GetImport	Accorde l'autorisation de récupérer des informations sur une tâche d'importation spécifique	Lecture			
GetInsightSelectors	Accorde l'autorisation de répertorier les sélecteurs CloudTrail Insights configurés pour un magasin de données de parcours ou d'événements	Lecture	eventdatastore trail		
GetQueryResults	Accorde l'autorisation de récupérer les résultats d'une requête terminée	Lecture	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetResourcePolicy		Lecture	channel		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation d'obtenir la politique de ressource attachée à un secret		dashboard		
			eventdatastore		
GetServiceLinkedChannel [autorisation uniquement]	Accorde l'autorisation de répertorier les paramètres du canal lié à un service	Lecture	channel*		
GetTrail	Accorde l'autorisation de répertorier les paramètres du journal d'activité	Lecture	trail*		
GetTrailStatus	Accorde l'autorisation de récupérer la liste au format JSON des informations sur le journal d'activité spécifié	Lecture	trail*		
ListChannels	Accorde l'autorisation de répertorier les chaînes dans le compte actuel et leurs noms sources	List			
ListDashboards	Autorise votre compte à répertorier les tableaux de bord associés à la région actuelle	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEventDataStores	Accorde l'autorisation de répertorier les magasins de données d'événement associés à la région actuelle de votre compte	List			
ListImportFailures	Accorde l'autorisation de renvoyer une liste d'échecs pour l'importation spécifiée	Lecture			
ListImports	Accorde l'autorisation de renvoyer des informations sur toutes les importations, ou sur un ensemble sélectionné d'importations par ImportStatus ou par destination	List			
ListInsightsData	Accorde l'autorisation de récupérer les données capturées par CloudTrail Insights	List	trail*		
ListPublicKeys	Accorde l'autorisation de répertorier les clés publiques dont les clés privées ont été utilisées pour signer les fichiers de journal d'activité dans un laps de temps spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListQueries	Accorde l'autorisation de répertorier les requêtes associées à un magasin de données d'événement	List	eventdatastore*		
ListServiceLinkedChannels [autorisation uniquement]	Accorde l'autorisation de répertorier les canaux liés aux services associés à la région actuelle pour un compte spécifié	List			
ListTags	Autorise à répertorier les balises pour les sentiers, les magasins de données d'événements, les chaînes ou les tableaux de bord de la région actuelle	Lecture	channel		
			dashboard		
			eventdatastore		
			trail		
ListTrails	Accorde l'autorisation de répertorier les journaux d'activité associés à la région actuelle de votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
LookupEvents	Accorde l'autorisation de rechercher et de récupérer des données métriques pour les événements d'activité des API capturés par CloudTrail ceux qui créent, mettent à jour ou suppriment des ressources dans votre compte	Lecture			
PutEventConfiguration	Accorde l'autorisation de créer et de mettre à jour des configurations d'événements pour un parcours ou un magasin de données d'événements	Écrire	eventdatastore		iam:CreateServiceLinkedRole iam:GetRole
			trail		
PutEventSelectors	Accorde l'autorisation de créer et mettre à jour les sélecteurs d'événements pour un journal d'activité	Écrire	trail*		
PutInsightSelectors	Autorise la création et la mise à jour CloudTrail des sélecteurs Insights pour un magasin de données de parcours ou d'événements	Écrire	eventdatastore		
			trail		
PutResourcePolicy	Accorde l'autorisation d'attacher une politique de ressource à un secret	Écrire	channel		
			dashboard		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			eventdatastore		
RegisterOrganizationDelegatedAdmin	Accorde l'autorisation d'enregistrer un compte membre d' AWS Organizations en tant qu'administrateur délégué	Écrire			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator
RemoveTags	Autorise à supprimer des balises d'un parcours, d'une banque de données d'événements, d'une chaîne ou d'un tableau de bord	Identification	channel		
			dashboard		
			eventdatastore		
			trail		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
RestoreEventDataStore	Accorde l'autorisation de restaurer un magasin de données d'événement	Écrire	eventdatastore*		
SearchSampleQueries	Accorde l'autorisation d'effectuer une recherche sémantique pour les exemples de CloudTrail requêtes Lake	Lecture			
StartDashboardRefresh	Accorde l'autorisation de démarrer une actualisation sur le tableau de bord spécifié	Écrire	dashboard*		cloudtrail:StartQuery
StartEventDataStoreIngestion	Accorde l'autorisation de démarrer l'ingestion sur un magasin de données d'événement	Écrire	eventdatastore*		
StartImport	Accorde l'autorisation de démarrer une importation d'événements de suivi enregistrés depuis un compartiment S3 source vers un magasin de données d'événements de destination	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartLogging	Accorde l'autorisation de démarrer l'enregistrement des appels d' AWS API et la livraison des fichiers journaux pour un suivi	Écrire	trail*		
StartQuery	Accorde l'autorisation de démarrer une nouvelle requête sur un magasin de données d'événement spécifié	Écrire	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	Accorde l'autorisation de d'arrêter l'ingestion sur un magasin de données d'événement	Écrire	eventdatastore*		
StopImport	Accorde l'autorisation d'arrêter une importation spécifiée	Écrire			
StopLogging	Autorise l'arrêt de l'enregistrement des appels d' AWS API et de la livraison des fichiers journaux pour un suivi	Écrire	trail*		
UpdateChannel	Accorde l'autorisation de mettre à jour un canal.	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDashboard	Accorde l'autorisation de mettre à jour un tableau de bord	Écrire	dashboard*		cloudtrail:StartDashboardRefresh cloudtrail:StartQuery
UpdateEventDataStore	Accorde l'autorisation de mettre à jour un magasin de données d'événement	Écrire	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateServiceLinkedChannel [autorisation uniquement]	Accorde l'autorisation de mettre à jour les paramètres des canaux liés au service pour la livraison des données de journal à un service AWS	Écrire	channel*		
UpdateTrail	Accorde l'autorisation de mettre à jour les paramètres qui spécifient la livraison de fichiers journaux	Écrire	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Types de ressources définis par AWS CloudTrail

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> Pour les politiques qui contrôlent l'accès aux CloudTrail actions, l'élément Ressource est toujours défini sur « * ». Pour plus d'informations sur l'utilisation des ressources ARNs dans une politique IAM, voir Comment AWS CloudTrail fonctionne avec IAM dans le guide de l'AWS CloudTrail utilisateur.

Types de ressources	ARN	Clés de condition
trail	`arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}`	aws:ResourceTag/${TagKey}
eventdatastore	`arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/${EventDataStoreId}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/${DashboardName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS CloudTrail

AWS CloudTrail définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString

Actions, ressources et clés de condition pour les AWS CloudTrail données

AWS CloudTrail Les données (préfixe de service :`cloudtrail-data`) fournissent les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CloudTrail Data
- Types de ressources définis par AWS CloudTrail Data
- Clés de condition pour les AWS CloudTrail données

Actions définies par AWS CloudTrail Data

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutAuditEvents	Accorde l'autorisation d'ingérer les événements de votre application dans Lake CloudTrail	Écrire	channel*		

Types de ressources définis par AWS CloudTrail Data

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> Pour les politiques qui contrôlent l'accès aux CloudTrail actions, l'élément Ressource est toujours défini sur « * ». Pour plus d'informations sur l'utilisation des ressources ARNs dans une politique IAM, voir Comment AWS CloudTrail fonctionne avec IAM dans le guide de l'AWS CloudTrail utilisateur.

Types de ressources	ARN	Clés de condition
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les AWS CloudTrail données

AWS CloudTrail Data définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur de balise dans la demande	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch

Amazon CloudWatch (préfixe de service :`cloudwatch`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch

- Types de ressources définis par Amazon CloudWatch
- Clés de condition pour Amazon CloudWatch

Actions définies par Amazon CloudWatch

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetServiceLevelIndicatorReport	Octroie l'autorisation d'obtenir par lots des rapports sur les indicateurs de niveau de service.	Lecture			
BatchGetServiceLevelObjectiveBudgetReport	Octroie l'autorisation de récupérer par lots des rapports budgétaires sur les objectifs de niveau de service.	Lecture	slo*		
CreateServiceLevelObjective	Octroie l'autorisation de créer un objectif de niveau de service.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarmMuteRule	Autorise la suppression d'une règle de désactivation d'une alarme	Écrire	alarm-mute-rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAlarms	Accorde l'autorisation de supprimer un ensemble d'alarmes.	Écriture	alarm*		
DeleteAnomalyDetector	Accorde l'autorisation de supprimer de votre compte le modèle de détection d'anomalies spécifié.	Écrire			
DeleteDashboards	Accorde l'autorisation de supprimer tous les CloudWatch tableaux de bord que vous spécifiez	Écrire	dashboard*		
DeleteInsightRules	Accorde l'autorisation de supprimer un ensemble de règles Insight.	Écrire	insight-rule*		
DeleteMetricStream	Accorde l'autorisation de supprimer le flux CloudWatch métrique que vous spécifiez	Écrire	metric-stream*		
DeleteServiceLevelObjective	Octroie l'autorisation de supprimer un objectif de niveau de service.	Écrire	slo*		
DescribeAlarmHistory	Accorde l'autorisation de récupérer l'historique de l'alarme spécifiée.	Lecture	alarm*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAlarms	Accorde l'autorisation de décrire toutes les alarmes, actuellement détenues par le compte de l'utilisateur.	Lecture	alarm*		
DescribeAlarmsForMetric	Accorde l'autorisation de décrire toutes les alarmes configurées sur la métrique spécifiée, actuellement détenue par le compte de l'utilisateur.	Lecture			
DescribeAnomalyDetectors	Accorde l'autorisation de lister les modèles de détection d'anomalies que vous avez créés dans votre compte.	Lecture			
DescribeInsightRules	Accorde l'autorisation de décrire toutes les règles Insight, actuellement détenues par le compte de l'utilisateur.	Lecture			
DisableAlarmActions	Accorde l'autorisation de désactiver des actions d'un ensemble d'alarmes.	Écriture	alarm*		
DisableInsightRules	Accorde l'autorisation de désactiver un ensemble de règles Insight.	Écriture	insight-rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableAlarmActions	Accorde l'autorisation d'activer des actions pour un ensemble d'alarmes.	Écriture	alarm*		
EnableInsightRules	Accorde l'autorisation d'activer un ensemble de règles Insight.	Écrire	insight-rule*		
EnableTopologyDiscovery	Accorde l'autorisation d'activer la découverte d'une CloudWatch topologie	Écrire			
GenerateQuery	Octroie l'autorisation de générer une chaîne de demande Metrics Insights ou Logs Insights à partir d'une invite en langage naturel.	Lecture			
GenerateQueryResultsSummary	Accorde l'autorisation de générer un résumé des résultats des CloudWatch LogInsights requêtes en langage naturel à l'aide de l'IA générative	Lecture			
GetAlarmMuteRule	Accorde l'autorisation d'obtenir une règle de désactivation des alarmes	Lecture	alarm-mute-rule*		
GetDashboard	Accorde l'autorisation d'afficher les détails du CloudWatch tableau de bord que vous spécifiez	Lecture	dashboard*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInsightRuleReport	Accorde l'autorisation de renvoyer le rapport Top_N des contributeurs uniques sur une plage de temps pour une règle Insight donnée.	Lecture	insight-rule*		
GetMetricData	Permet de récupérer des quantités par lots de données CloudWatch métriques et d'effectuer des calculs métriques sur les données récupérées	Lecture			
GetMetricStatistics	Accorde l'autorisation d'extraire des statistiques pour la métrique spécifiée.	Lecture			
GetMetricStream	Autorise le renvoi des détails d'un flux CloudWatch métrique	Lecture	metric-stream*		
GetMetricWidgetImage	Accorde l'autorisation de récupérer des instantanés de widgets de métrique.	Lecture			
GetService	Octroie l'autorisation de récupérer des informations sur un service.	Lecture	service*		
GetServiceData [autorisation uniquement]	Octroie l'autorisation de récupérer les données d'un service.	Lecture	service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceLevelObjective	Octroie l'autorisation de récupérer des informations sur un objectif de niveau de service.	Lecture	slo*		
GetTopologyDiscoveryStatus [autorisation uniquement]	Accorde l'autorisation de récupérer le statut de découverte d'une CloudWatch topologie	Lecture			
GetTopologyMap	Accorde l'autorisation de récupérer une CloudWatch carte topologique	Lecture			
Link [autorisation uniquement]	Accorde l'autorisation de partager CloudWatch des ressources avec un compte de surveillance	Écrire			
ListAlarmMuteRules	Accorde l'autorisation de récupérer une liste des règles de désactivation des alarmes détenues par le compte de l'utilisateur	List	alarm-mute-rule*		
ListDashboards	Autorise le renvoi d'une liste de tous les CloudWatch tableaux de bord de votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEntitiesForMetric [autorisation uniquement]	Accorde l'autorisation de récupérer toutes les entités qui émettent une métrique donnée	List			
ListManagedInsightRules	Accorde l'autorisation de répertorier les règles Insight gérées disponibles pour un ARN de ressource donné	Lecture		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
ListMetricStreams	Autorise le renvoi d'une liste de tous les flux CloudWatch métriques de votre compte	List			
ListMetrics	Accorde l'autorisation de récupérer une liste de métriques valides stockées pour le Compte AWS propriétaire	List			
ListServiceLevelObjectives	Octroie l'autorisation de répertorier des objectifs de niveau de service.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServices	Accorde l'autorisation de répertorier les services	List			
ListTagsForResource	Accorde l'autorisation de répertorier les tags d'une CloudWatch ressource Amazon	List	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
	SCÉNARIO : CloudWatch-Alarm		alarm*		
	SCÉNARIO : CloudWatch-AlarmMuteRule		alarm-mute-rule*		
	SCÉNARIO : CloudWatch-InsightRule		insight-rule*		
	SCÉNARIO : CloudWatch-ServiceLevelObjective		slo*		
PutAlarmMuteRule	Autorise la création ou la mise à jour d'une règle de désactivation des alarmes	Écrire	alarm-mute-rule*		
			alarm		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
PutAnomalyDetector	Autorise la création ou la mise à jour d'un modèle de détection des anomalies pour une métrique CloudWatch	Écrire			
PutCompositeAlarm	Accorde l'autorisation de créer ou de mettre à jour une alarme composite.	Écrire	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutDashboard	Accorde l'autorisation de créer un CloudWatch tableau de bord ou de mettre à jour un tableau de bord existant s'il existe déjà	Écrire	dashboard*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutInsightRule	Accorde l'autorisation de créer une nouvelle règle Insight ou de remplacer une règle Insight existante.	Écrire	insight-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	
PutManagedInsightRules	Accorde l'autorisation de créer des règles Insight gérées	Écrire		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
PutMetricAlarm	Accorde l'autorisation de créer ou de mettre à jour une alarme et l'associe à la CloudWatch métrique Amazon spécifiée	Écrire	alarm*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	Autorise la publication de points de données métriques sur Amazon CloudWatch	Écrire		cloudwatch:namespace	
PutMetricStream	Autorise la création d'un flux CloudWatch métrique ou la mise à jour d'un flux métrique existant s'il existe déjà	Écrire	metric-stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SetAlarmState	Accorde l'autorisation de définir temporairement l'état d'une alarme à des fins de test.	Écrire	alarm*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMetricStreams	Accorde l'autorisation de démarrer tous les flux CloudWatch métriques que vous spécifiez	Écrire	metric-stream*		
StopMetricStreams	Accorde l'autorisation d'arrêter tous les flux CloudWatch métriques que vous spécifiez	Écrire	metric-stream*		
TagResource	Accorde l'autorisation d'ajouter des balises à une CloudWatch ressource Amazon	Identification	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
				aws:TagKeys aws:RequestTag/${TagKey}	
	SCÉNARIO : CloudWatch-Alarm		alarm*		
	SCÉNARIO : CloudWatch-AlarmMuteRule		alarm-mute-rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	SCÉNARIO : CloudWatch-InsightRule		insight-rule*		
	SCÉNARIO : CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Accorde l'autorisation de supprimer un tag d'une CloudWatch ressource Amazon	Identification	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
				aws:TagKeys	
	SCÉNARIO : CloudWatch-Alarm		alarm*		
	SCÉNARIO : CloudWatch-AlarmMuteRule		alarm-mute-rule*		
	SCÉNARIO : CloudWatch-InsightRule		insight-rule*		
	SCÉNARIO : CloudWatch-ServiceLevelObjective		slo*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateServiceLevelObjective	Octroie l'autorisation de mettre à jour un objectif de niveau de service.	Écrire	slo*		

Types de ressources définis par Amazon CloudWatch

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
alarm	`arn:${Partition}:cloudwatch:${Region}:${Account}:alarm:${AlarmName}`	aws:ResourceTag/${TagKey}
alarm-mute-rule	`arn:${Partition}:cloudwatch:${Region}:${Account}:alarm-mute-rule:${AlarmMuteRuleName}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:cloudwatch::${Account}:dashboard/${DashboardName}`	
insight-rule	`arn:${Partition}:cloudwatch:${Region}:${Account}:insight-rule/${InsightRuleName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
metric-stream	arn:${Partition}:cloudwatch:${Region}:${Account}:metric-stream/${MetricStreamName}	aws:ResourceTag/${TagKey}
slo	arn:${Partition}:cloudwatch:${Region}:${Account}:slo/${SloName}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:cloudwatch:${Region}:${Account}:service/${ServiceName}-${UniqueAttributesHex}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch

Amazon CloudWatch définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de l'ensemble des valeurs autorisées pour chacune des balises.	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur de balise associée à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString
cloudwatch:AlarmActions	Filtre les actions en fonction des actions d'alarme définies	ArrayOfString

Clés de condition	Description	Type
cloudwatch:namespace	Filtre les actions en fonction de la présence de valeurs d'espace de noms facultatives	String
cloudwatch:requestInsightRuleLogGroups	Filtre les actions en fonction des groupes de journaux spécifiés dans une règle Insight	ArrayOfString
cloudwatch:requestManagedResourceARNs	Filtre l'accès en fonction de la ressource ARNs spécifiée dans une règle Insight gérée	ArrayOfARN

Actions, ressources et clés de condition pour Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights (préfixe de service :`applicationinsights`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Application Insights
- Types de ressources définis par Amazon CloudWatch Application Insights
- Clés de condition pour Amazon CloudWatch Application Insights

Actions définies par Amazon CloudWatch Application Insights

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddWorkload	Octroie l'autorisation d'ajouter une charge de travail.	Écrire			
CreateApplication	Accorde l'autorisation de créer une application à partir d'un groupe de ressources	Écriture			
CreateComponent	Accorde l'autorisation de créer un composant à partir d'un groupe de ressources	Écriture			
CreateLogPattern	Accorde l'autorisation de créer un modèle de journal	Écriture			
DeleteApplication	Accorde l'autorisation de supprimer une application	Écriture			
DeleteComponent	Accorde l'autorisation de supprimer un composant	Écriture			
DeleteLogPattern	Accorde l'autorisation de supprimer un modèle de journal	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeApplication	Accorde l'autorisation de décrire une application	Lecture			
DescribeComponent	Accorde l'autorisation de décrire un composant	Lecture			
DescribeComponentConfiguration	Accorde l'autorisation de décrire la configuration d'un composant	Lecture			
DescribeComponentConfigurationRecommendation	Accorde l'autorisation de décrire la configuration recommandée du composant d'application	Lecture			
DescribeLogPattern	Accorde l'autorisation de décrire un modèle de journal	Lecture			
DescribeObservation	Accorde l'autorisation de décrire une observation	Lecture			
DescribeProblem	Accorde l'autorisation de décrire un problème	Lecture			
DescribeProblemObservations	Accorde l'autorisation de décrire l'observation dans un problème	Lecture			
DescribeWorkload	Octroie l'autorisation de décrire une charge de travail.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Link [autorisation uniquement]	Accorde l'autorisation de partager des ressources Application Insights avec un compte de surveillance	Écrire			
ListApplications	Accorde l'autorisation de répertorier toutes les applications	Liste			
ListComponents	Accorde l'autorisation de répertorier les composants d'une application	Liste			
ListConfigurationHistory	Accorde l'autorisation de répertorier l'historique de configuration	Liste			
ListLogPatternSets	Accorde l'autorisation de répertorier les jeux de modèles de journal d'une application	Liste			
ListLogPatterns	Accorde l'autorisation de répertorier les modèles de journaux	Liste			
ListProblems	Accorde l'autorisation de répertorier les problèmes dans une application	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture			
ListWorkloads	Accorde l'autorisation de répertorier les charges de travail	List			
RemoveWorkload	Octroie l'autorisation de supprimer une charge de travail.	Écrire			
TagResource	Accorde l'autorisation de baliser une ressource	Balisage		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage		aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écriture			
UpdateComponent	Accorde l'autorisation de mettre à jour un composant	Écriture			
UpdateComponentConfiguration	Accorde l'autorisation de mettre à jour la configuration d'un composant	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateLogPattern	Accorde l'autorisation de mettre à jour un modèle de journal	Écrire			
UpdateProblem	Octroie l'autorisation de mettre à jour un problème.	Écrire			
UpdateWorkload	Octroie l'autorisation de mettre à jour une charge de travail.	Écrire			

Types de ressources définis par Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon CloudWatch Application Insights, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch Application Signals

Amazon CloudWatch Application Signals (préfixe de service :`application-signals`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Application Signals
- Types de ressources définis par Amazon CloudWatch Application Signals
- Clés de condition pour Amazon CloudWatch Application Signals

Actions définies par Amazon CloudWatch Application Signals

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetServiceLevelObjectiveBudgetReport	Octroie l'autorisation de récupérer par lots des rapports budgétaires sur les objectifs de niveau de service.	Lecture	slo*		
BatchUpdateExclusionWindows	Accorde l'autorisation d'ajouter ou de supprimer des fenêtres d'exclusion sur Amazon CloudWatch SLOs	Écrire	slo*		
CreateServiceLevelObjective	Octroie l'autorisation de créer un objectif de niveau de service.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroupingConfiguration	Accorde l'autorisation de supprimer une configuration de regroupement	Écrire			
DeleteServiceLevelObjective	Octroie l'autorisation de supprimer un objectif de niveau de service.	Écrire	slo*		
GetService	Octroie l'autorisation de récupérer des informations sur un service.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceLevelObjective	Octroie l'autorisation de récupérer des informations sur un objectif de niveau de service.	Lecture	slo*		
Link [autorisation uniquement]	Autorise le partage des ressources des signaux d'application avec un compte de surveillance	Écrire			
ListAuditFindings	Accorde l'autorisation de répertorier les résultats d'audit des services	List			
ListEntityEvents	Accorde l'autorisation de répertorier des événements pour une entité	List			
ListGroupingAttributeDefinitions	Accorde l'autorisation de répertorier les configurations d'attributs de regroupement	List			
ListObservedEntities	Accorde l'autorisation de répertorier les entités associées à d'autres entités	List			
ListServiceDependencies	Accorde l'autorisation de répertorier les dépendances des services	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceDependents	Accorde l'autorisation de répertorier les personnes dépendantes du service	Lecture			
ListServiceLevelObjectiveExclusionWindows	Accorde l'autorisation de répertorier les fenêtres d'exclusion pour un Amazon CloudWatch SLO	List	slo*		
ListServiceLevelObjectives	Octroie l'autorisation de répertorier des objectifs de niveau de service.	List			
ListServiceOperations	Accorde l'autorisation de répertorier les opérations de service	Lecture			
ListServiceStates	Accorde l'autorisation de répertorier les états de service	List			
ListServices	Accorde l'autorisation de répertorier les services	List			
ListTagsForResource	Accorde l'autorisation de répertorier les tags pour un Amazon CloudWatch SLO	Lecture	slo*		
PutGroupingConfiguration	Accorde l'autorisation de créer ou de mettre à jour une configuration de regroupement	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDiscovery	Accorde l'autorisation d'activer CloudWatch la découverte	Écrire			
TagResource	Accorde l'autorisation d'ajouter des tags à un Amazon CloudWatch SLO	Identification	slo*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Autorise le débalisage d'un Amazon SLO CloudWatch	Identification	slo*		
				aws:TagKeys	
UpdateServiceLevelObjective	Octroie l'autorisation de mettre à jour un objectif de niveau de service.	Écrire	slo*		

Types de ressources définis par Amazon CloudWatch Application Signals

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
slo	`arn:${Partition}:application-signals:${Region}:${Account}:slo/${SloName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch Application Signals

Amazon CloudWatch Application Signals définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch Evidently

Amazon CloudWatch Evidently (préfixe de service :`evidently`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Evidently
- Types de ressources définis par Amazon CloudWatch Evidently
- Clés de condition pour Amazon CloudWatch Evidently

Actions définies par Amazon CloudWatch Evidently

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchEvaluateFeature	Accorde l'autorisation d'envoyer une requête de fonction d'évaluation en lot.	Écrire	Feature*		
CreateExperiment	Accorde l'autorisation de créer une expérience	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFeature	Accorde l'autorisation de créer une fonction	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunch	Accorde l'autorisation de créer un lancement.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Accorde l'autorisation de créer un projet	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:GetRole
CreateSegment	Accorde l'autorisation de créer un segment	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExperiment	Accorde l'autorisation de supprimer une expérience	Écrire	Experiment*		
DeleteFeature	Accorde l'autorisation de supprimer une fonction	Écrire	Feature*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLaunch	Accorde l'autorisation de supprimer un lancement.	Écrire	Launch*		
DeleteProject	Accorde l'autorisation de supprimer un projet	Écrire	Project*		
DeleteSegment	Accorde l'autorisation de supprimer un segment	Écrire	Segment*		
EvaluateFeature	Accorde l'autorisation d'envoyer une requête de fonction d'évaluation.	Écrire	Feature*		
GetExperiment	Accorde l'autorisation d'obtenir les détails de l'expérience	Lecture	Experiment*		
GetExperimentResults	Accorde l'autorisation d'obtenir le résultat de l'expérience	Lecture	Experiment*		
GetFeature	Accorde l'autorisation d'obtenir les détails de la fonction	Lecture	Feature*		
GetLaunch	Accorde l'autorisation d'obtenir les détails du lancement	Lecture	Launch*		
GetProject	Accorde l'autorisation d'obtenir les détails du projet	Lecture	Project*		
GetSegment	Accorde l'autorisation d'obtenir les détails du segment	Lecture	Segment*		
ListExperiments	Accorde l'autorisation de répertorier les expériences	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFeatures	Accorde l'autorisation de répertorier les fonctions	Lecture			
ListLaunches	Accorde l'autorisation de répertorier les lancements	Lecture			
ListProjects	Accorde l'autorisation de répertorier les projets	Lecture			
ListSegmentReferences	Accorde l'autorisation de répertorier les ressources référençant un segment	Lecture			
ListSegments	Accorde l'autorisation de répertorier les segments	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises des ressources	Lecture			
PutProjectEvents	Accorde l'autorisation d'envoyer des événements de performance.	Écrire	Project*		
StartExperiment	Accorde l'autorisation de lancer une expérience	Écrire	Experiment*		
StartLaunch	Accorde l'autorisation de démarrer un lancement	Écrire	Launch*		
StopExperiment	Accorde l'autorisation d'arrêter une expérience	Écrire	Experiment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopLaunch	Accorde l'autorisation d'arrêter un lancement	Écrire	Launch*		
TagResource	Accorde l'autorisation de baliser des ressources	Identification	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestSegmentPattern	Accorde l'autorisation de tester un modèle de segment	Lecture			
UntagResource	Accorde l'autorisation d'annuler le balisage des ressources	Identification	Experiment		
			Feature		
			Launch		
			Project		
			Segment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateExperiment	Accorde l'autorisation de mettre à jour l'expérience	Écrire	Experiment*		
UpdateFeature	Octroie l'autorisation de mettre à jour la fonction	Écrire	Feature*		
UpdateLaunch	Accorde l'autorisation de mettre à jour un lancement.	Écrire	Launch*		
UpdateProject	Accorde l'autorisation de mettre à jour le projet	Écrire	Project*		iam:CreateServiceLinkedRole iam:GetRole
UpdateProjectDataDelivery	Accorde l'autorisation de mettre à jour la livraison de données du projet	Écrire	Project*		

Types de ressources définis par Amazon CloudWatch Evidently

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Project	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}`	aws:ResourceTag/${TagKey}
Feature	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/feature/${FeatureName}`	aws:ResourceTag/${TagKey}
Experiment	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/experiment/${ExperimentName}`	aws:ResourceTag/${TagKey}
Launch	`arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/launch/${LaunchName}`	aws:ResourceTag/${TagKey}
Segment	`arn:${Partition}:evidently:${Region}:${Account}:segment/${SegmentName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch Evidently

Amazon définit CloudWatch évidemment les clés de condition suivantes qui peuvent être utilisées dans le cadre d'`Condition`une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande pour le compte du principal IAM	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource qui effectue la demande pour le compte du principal IAM	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande pour le compte du principal IAM	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor (préfixe de service :`internetmonitor`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Internet Monitor
- Types de ressources définis par Amazon CloudWatch Internet Monitor
- Clés de condition pour Amazon CloudWatch Internet Monitor

Actions définies par Amazon CloudWatch Internet Monitor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMonitor	Accorde la permission de créer un moniteur	Écrire	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	Accorde la permission de supprimer un moniteur	Écrire	Monitor*		
GetHealthEvent	Accorde l'autorisation d'obtenir des informations sur un événement de santé pour un moniteur spécifié	Lecture	Monitor*		
GetInternetEvent	Accorde l'autorisation d'obtenir des informations sur un événement Internet spécifique	Lecture	InternetEvent*		
GetMonitor	Accorde l'autorisation d'obtenir des informations sur un moniteur	Lecture	Monitor*		
GetQueryResults	Accorde l'autorisation d'obtenir les résultats d'une requête de données pour un moniteur	Lecture	Monitor*		
GetQueryStatus	Accorde l'autorisation d'obtenir le statut d'une requête de données pour un moniteur	Lecture	Monitor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Link [autorisation uniquement]	Autorise le partage des ressources d'Internet Monitor avec un compte de surveillance	Écrire			
ListHealthEvents	Autorise la la la la création de la liste de tous les événements d'événements d'événements d'événements d'	List	Monitor*		
ListInternetEvents	Accorde l'autorisation de répertorier tous les événements Internet	List			
ListMonitors	Accorde l'autorisation de répertorier tous les moniteurs d'un compte et leurs statuts	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	Monitor*		
StartQuery	Accorde l'autorisation de lancer une requête de données pour un moniteur	Lecture	Monitor*		
StopQuery	Accorde l'autorisation d'arrêter une requête de données pour un moniteur	Lecture	Monitor*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource.	Balisage	Monitor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	Monitor*		
				aws:TagKeys	
UpdateMonitor	Accorde l'autorisation de mettre à jour un moniteur	Écrire	Monitor*		

Types de ressources définis par Amazon CloudWatch Internet Monitor

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
HealthEvent	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}/health-event/${EventId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Monitor	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
InternetEvent	`arn:${Partition}:internetmonitor::${Account}:internet-event/${InternetEventId}`	

Clés de condition pour Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de balise dans la requête.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch Logs

Amazon CloudWatch Logs (préfixe de service :`logs`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Logs
- Types de ressources définis par Amazon CloudWatch Logs
- Clés de condition pour Amazon CloudWatch Logs

Actions définies par Amazon CloudWatch Logs

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateKmsKey	Accorde l'autorisation d'associer la AWS clé principale du client (CMK) du service de gestion des clés (AWS KMS) spécifiée au groupe de journaux spécifié	Écrire	log-group *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateSourceToS3TableIntegration	Accorde l'autorisation d'associer une source de journal à une intégration de S3 Tables	Écrire			
CallWithBearerToken [autorisation uniquement]	Accorde l'autorisation d'authentifier les demandes à l'aide d'un jeton porteur	Écrire			
CancelExportTask	Accorde l'autorisation d'annuler une tâche d'exportation si elle affiche l'état PENDING ou RUNNING	Écrire			
CancelImportTask	Autorise l'annulation d'une importation de CloudTrail Lake vers CloudWatch	Écrire			
CreateDelivery	Accorde l'autorisation de créer une diffusion connectant une source de diffusion à une destination de diffusion	Écrire	delivery*		
			delivery-destination*		
			delivery-source*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportTask	Accorde l'autorisation de créer un ExportTask qui vous permet d'exporter efficacement les données d'un groupe de journaux vers votre compartiment Amazon S3	Écrire	log-group*		
CreateImportTask	Accorde l'autorisation de démarrer un processus asynchrone pour importer des données d'un magasin de données d'événements CloudTrail Lake vers un groupe de journaux géré dans CloudWatch	Écrire			
CreateLogAnomalyDetector	Octroie l'autorisation de créer un détecteur d'anomalies de journaux.	Écrire	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLogDelivery [autorisation uniquement]	Accorde l'autorisation de créer une diffusion de journaux	Écrire			
CreateLogGroup	Accorde l'autorisation de créer un groupe de journaux avec le nom spécifié	Écrire	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogStream	Accorde l'autorisation de créer un flux de journaux avec le nom spécifié	Écrire	log-stream*		
CreateLookupTable	Accorde l'autorisation de créer une table de recherche	Écrire	lookup-table*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateScheduledQuery	Accorde l'autorisation de créer une requête planifiée	Écrire	scheduled-query*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccountPolicy	Accorde l'autorisation de supprimer une politique de compte	Écrire			
DeleteDataProtectionPolicy	Accorde l'autorisation de supprimer une politique de protection des données attachée à un groupe de journaux	Écrire	log-group*		
DeleteDelivery	Accorde l'autorisation de supprimer une livraison	Écrire	delivery*		
DeleteDeliveryDestination	Accorde l'autorisation de supprimer une destination de livraison une fois toutes les livraisons associées supprimées	Écrire	delivery-destination*		
DeleteDeliveryDestinationPolicy	Accorde l'autorisation de supprimer une stratégie de destination de livraison associée à une destination de livraison	Écrire	delivery-destination*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDeliverySource	Accorde l'autorisation de supprimer une source de livraison une fois toutes les livraisons associées supprimées	Écrire	delivery-destination*		
DeleteDestination	Accorde l'autorisation de supprimer la destination avec le nom spécifié	Écrire	destination*		
DeleteIndexPolicy	Accorde l'autorisation de supprimer une politique d'index attachée à un groupe de journaux	Écrire			
DeleteIntegration	Accorde l'autorisation de supprimer l'intégration	Écrire			
DeleteLogAnomalyDetector	Octroie l'autorisation de supprimer un détecteur d'anomalies de journaux.	Écrire	anomaly-detector*		
DeleteLogDelivery [autorisation uniquement]	Accorde l'autorisation de supprimer les informations de livraison de journaux pour la livraison de journaux spécifiée	Écrire			
DeleteLogGroup	Accorde l'autorisation de supprimer le groupe de journaux avec le nom spécifié	Écrire	log-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLogStream	Accorde l'autorisation de supprimer un flux de journaux	Écrire	log-stream*		
DeleteLookupTable	Autorise la suppression d'une table de recherche	Écrire	lookup-table*		
DeleteMetricFilter	Accorde l'autorisation de supprimer un filtre de métrique associé au groupe de journaux spécifié	Écrire	log-group*		
DeletePipelineRule [autorisation uniquement]	Autorise la suppression du pipeline de télémétrie	Écrire			
DeleteQueryDefinition	Autorise la suppression d'une définition de requête CloudWatch Logs Insights enregistrée	Écrire			
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource dans ce compte	Gestion des autorisations			
DeleteRetentionPolicy	Accorde l'autorisation de supprimer la politique de conservation du groupe de journaux spécifié	Écrire	log-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteScheduledQuery	Accorde l'autorisation de supprimer une requête planifiée	Écrire	scheduled-query*		
DeleteSubscriptionFilter	Accorde l'autorisation de supprimer un filtre d'abonnement associé au groupe de journaux spécifié	Écrire	log-group*		
DeleteTransformer	Accorde l'autorisation de supprimer un transformateur associé au groupe de journaux spécifié	Écrire	log-group*		
DescribeAccountPolicies	Accorde l'autorisation de récupérer les politiques du compte	List			
DescribeConfigurationTemplates	Accorde l'autorisation de récupérer une liste de modèles de configuration des types de journaux disponibles	List			
DescribeDeliveries	Accorde l'autorisation de récupérer une liste de livraisons dans un compte	List			
DescribeDeliveryDestinations	Accorde l'autorisation de récupérer une liste de destinations de livraison dans un compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDeliverySources	Accorde l'autorisation de récupérer une liste de sources de livraison dans un compte	List			
DescribeDestinations	Accorde l'autorisation de renvoyer toutes les destinations associées Compte AWS à la demande	List			
DescribeExportTasks	Accorde l'autorisation de renvoyer toutes les tâches d'exportation associées Compte AWS à la demande	List			
DescribeFieldIndexes	Accorde l'autorisation de renvoyer tous les attributs d'indexation attachés aux groupes de journaux	List			
DescribeImportTaskBatches	Accorde l'autorisation de renvoyer des informations détaillées sur les lots individuels d'une tâche d'importation, y compris le statut et toute erreur	List			
DescribeImportTasks	Accorde l'autorisation de renvoyer toutes les tâches d'importation associées Compte AWS à la demande	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeIndexPolicies	Accorde l'autorisation de renvoyer toutes les politiques d'index associées aux groupes de journaux	List			
DescribeLogGroups	Accorde l'autorisation de renvoyer tous les groupes de journaux associés Compte AWS à la demande	List			
DescribeLogStreams	Accorde l'autorisation de renvoyer tous les flux de journaux associés au groupe de journaux spécifié	List	log-group *		
DescribeLookupTables	Autorise le renvoi de toutes les tables de recherche	List			
DescribeMetricFilters	Accorde l'autorisation de renvoyer tous les filtres de métriques associés au groupe de journaux spécifié	List	log-group *		
DescribeQueries	Accorde l'autorisation de renvoyer une liste de requêtes CloudWatch Logs Insights planifiées, exécutées ou exécutées récemment dans ce compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeQueryDefinitions	Accorde l'autorisation de renvoyer une liste paginée de vos définitions de requêtes CloudWatch Logs Insights enregistrées	List			
DescribeResourcePolicies	Accorde l'autorisation pour renvoyer toutes les politiques de ressources de ce compte	List			
DescribeSubscriptionFilters	Accorde l'autorisation de renvoyer tous les filtres d'abonnement associés au groupe de journaux spécifié	List	log-group *		
DisassociateKmsKey	Accorde l'autorisation de dissocier la AWS clé principale du client (CMK) associée du service de gestion des clés (AWS KMS) du groupe de journaux spécifié	Écrire	log-group *		
DisassociateSourceFromS3TableIntegration	Accorde l'autorisation de dissocier une source de journal d'une intégration S3 Tables	Écrire			
FilterLogEvents	Accorde l'autorisation d'extraire les événements de journaux, éventuellement filtrés par un modèle de filtre, du groupe de journaux spécifié	Lecture	log-group *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataProtectionPolicy	Accorde l'autorisation de récupérer une politique de protection des données attachée à un groupe de journaux	Lecture	log-group*		
GetDelivery	Accorde l'autorisation de récupérer une livraison unique	Lecture	delivery*		
GetDeliveryDestination	Accorde l'autorisation de récupérer une destination de livraison unique	Lecture	delivery-destination*		
GetDeliveryDestinationPolicy	Accorde l'autorisation de récupérer une stratégie de destination de livraison attachée à une destination de livraison	Lecture	delivery-destination*		
GetDeliverySource	Accorde l'autorisation de récupérer une source de livraison unique	Lecture	delivery-source*		
GetIntegration	Accorde l'autorisation de récupérer une seule intégration	Lecture			
GetLogAnomalyDetector	Octroie l'autorisation d'obtenir un détecteur d'anomalies de journaux.	Lecture	anomaly-detector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLogDelivery [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations de livraison de journal pour la livraison de journal spécifiée	Lecture			
GetLogEvents	Accorde l'autorisation de récupérer les événements de journaux du flux de journaux spécifié	Lecture	log-stream*		
GetLogFields	Accorde l'autorisation de récupérer une liste de champs de journal pour une source de données	Lecture			
GetLogGroupFields	Accorde l'autorisation de renvoyer la liste des champs inclus dans les événements de journaux dans le groupe de journaux spécifié, ainsi que le pourcentage d'événements de journaux contenant chaque champ	Lecture	log-group*		
GetLogRecord	Accorde l'autorisation de récupérer tous les champs et les valeurs d'un événement de journal unique	Lecture	log-group*		
GetLookupTable	Accorde l'autorisation de récupérer une table de recherche	Lecture	lookup-table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQueryResults	Accorde l'autorisation pour retourner les résultats de la requête spécifiée	Lecture	log-group*		
GetScheduledQuery	Accorde l'autorisation de récupérer les informations relatives à une requête planifiée spécifiée	Lecture	scheduled-query*		
GetScheduledQueryHistory	Accorde l'autorisation de renvoyer l'historique d'exécution pour une requête planifiée spécifiée	Lecture	scheduled-query*		
GetTransformer	Accorde l'autorisation de renvoyer le transformateur associé au groupe de journaux spécifié	Lecture	log-group*		
IntegrateWithS3Table [autorisation uniquement]	Accorde l'autorisation de transmettre les événements du journal aux tables S3	Écrire	log-group*		
Link [autorisation uniquement]	Accorde l'autorisation de partager CloudWatch des ressources avec un compte de surveillance	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAggregateLogGroupSummaries	Accorde l'autorisation de renvoyer un résumé agrégé de tous les groupes de journaux de la région, regroupés selon les caractéristiques de source de données spécifiées	List			
ListAnomalies	Permet de répertorier toutes les anomalies détectées lors Compte AWS de la demande	List	anomaly-detector		
ListEntitiesForLogGroup [autorisation uniquement]	Accorde l'autorisation de récupérer toutes les entités associées au groupe de journaux	List			
ListIntegrations	Accorde l'autorisation de répertorier toutes les intégrations associées à Compte AWS la demande	List			
ListLogAnomalyDetectors	Autorise le renvoi de tous les détecteurs d'anomalies associés à Compte AWS la demande	List	anomaly-detector		
ListLogDeliveries [autorisation uniquement]	Accorde l'autorisation de répertorier toutes les livraisons de journaux pour une source de and/or journal de compte spécifiée	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLogGroups	Accorde l'autorisation de renvoyer tous les groupes de journaux associés Compte AWS à la demande	List			
ListLogGroupsForEntity [autorisation uniquement]	Accorde l'autorisation de récupérer tous les groupes de journaux associés à l'entité	List			
ListLogGroupsForQuery	Accorde l'autorisation de renvoyer tous les groupes de journaux associés à la requête spécifiée	List			
ListScheduledQueries	Accorde l'autorisation de renvoyer toutes les requêtes planifiées associées à la Compte AWS formulation de la demande	List			
ListSourcesForS3TableIntegration	Accorde l'autorisation de renvoyer toutes les sources de journaux associées à une intégration de S3 Tables	List			
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée	List	anomaly-detector		
			delivery		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			delivery-destination		
			delivery-source		
			destination		
			log-group		
			lookup-table		
ListTagsLogGroup	Accorde l'autorisation de répertorier les balises pour le groupe de journaux spécifié	List	log-group *		
ProcessWithPipeline [autorisation uniquement]	Autorise le traitement et la transformation des événements du journal par le biais de transformateurs de pipeline avant le stockage	Écrire	log-group *		
PutAccountPolicy	Accorde l'autorisation de joindre une politique de compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutBearerTokenAuthentication	Accorde l'autorisation d'activer ou de désactiver l'authentification basée sur un jeton porteur pour le groupe de journaux spécifié	Écrire	log-group*		
PutDataProtectionPolicy	Accorde l'autorisation de joindre une politique de protection des données afin de détecter et de supprimer les informations sensibles des événements du journal	Écrire	log-group*		
PutDeliveryDestination	Accorde l'autorisation à create/update une destination de livraison	Écrire	delivery-destination*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDeliveryDestinationPolicy	Accorde l'autorisation d'attacher une stratégie de destination de livraison à une destination de livraison	Écrire	delivery-destination*		
PutDeliverySource	Accorde l'autorisation à create/update une source de diffusion	Écrire	delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	
PutDestination	Accorde l'autorisation de créer ou de mettre à jour une destination	Écrire	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDestinationPolicy	Accorde l'autorisation de créer ou de mettre à jour une stratégie d'accès associée à une destination existante	Écrire	destination*		
PutIndexPolicy	Accorde l'autorisation d'associer une politique d'index au niveau du groupe de journaux afin d'optimiser la recherche et les requêtes	Écrire			
PutIntegration	Accorde l'autorisation de créer une intégration entre Cloudwatch Logs et OpenSearch	Écrire			
PutLogEvents	Accorde l'autorisation de charger un lot d'événements de journaux dans le flux de journaux spécifié	Écrire	log-stream*		
PutLogGroupDeletionProtection	Accorde l'autorisation d'activer ou de désactiver la protection contre la suppression pour le groupe de journaux spécifié	Écrire	log-group*		
PutMetricFilter	Accorde l'autorisation de créer ou de mettre à jour un filtre de métrique et de l'associer au groupe de journaux spécifié	Écrire	log-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutPipelineRule [autorisation uniquement]	Autorise la création d'un pipeline de télémétrie	Écrire			
PutQueryDefinition	Accorde l'autorisation de créer ou de mettre à jour une définition de requête	Écrire			
PutResourcePolicy	Accorde l'autorisation de créer ou de mettre à jour une politique de ressources autorisant d'autres AWS services à enregistrer des événements sur ce compte	Gestion des autorisations			
PutRetentionPolicy	Accorde l'autorisation pour définir la conservation du groupe de journaux spécifié	Écrire	log-group *		
PutSubscriptionFilter	Accorde l'autorisation de créer ou de mettre à jour un filtre d'abonnement et de l'associer au groupe de journaux spécifié	Écrire	log-group *		iam:PassRole
			destination		
PutTransformer	Accorde l'autorisation de créer ou de mettre à jour un transformateur et l'associe au groupe de journaux spécifié	Écrire	log-group *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartLiveTail	Accorde l'autorisation de démarrer une session Live Tail dans CloudWatch Logs	Lecture	log-group *		
StartQuery	Accorde l'autorisation de planifier une requête auprès d'un groupe de journaux à l'aide de CloudWatch Logs Insights	Lecture	log-group *		
StopLiveTail [autorisation uniquement]	Accorde l'autorisation d'arrêter une session Live Tail en cours	Lecture			
StopQuery	Autorise l'arrêt d'une requête CloudWatch Logs Insights en cours	Lecture			
TagLogGroup	Accorde l'autorisation d'ajouter ou de mettre à jour les balises spécifiées pour le groupe de journaux spécifié	Identification	log-group *		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour les balises spécifiées pour la ressource spécifiée	Identification	anomaly-detector		
			delivery		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			delivery-destination		
			delivery-source		
			destination		
			log-group		
			lookup-table		
			scheduled-query		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMetricFilter	Accorde l'autorisation de tester le modèle de filtre d'un filtre de métrique sur un exemple de messages d'événements de journaux	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestTransformer	Accorde l'autorisation de tester le transformateur par rapport à un échantillon de messages d'événements du journal	Lecture			
Unmask [autorisation uniquement]	Accorde l'autorisation de récupérer les événements de journaux démasqués qui ont été supprimés par une politique de protection des données	Lecture	log-group *		
UntagLogGroup	Accorde l'autorisation de supprimer les balises spécifiées du groupe de journaux spécifié	Identification	log-group *		
				aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de la ressource spécifiée	Identification	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			log-group		
			lookup-table		
			scheduled-query		
				aws:TagKeys	
UpdateAnomaly	Octroie l'autorisation de mettre à jour une anomalie signalée par un détecteur d'anomalies de journaux.	Écrire	anomaly-detector*		
UpdateDeliveryConfiguration	Accorde l'autorisation de mettre à jour la configuration associée à une livraison	Écrire	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateLogAnomalyDetector	Octroie l'autorisation de mettre à jour un détecteur d'anomalies de journaux.	Écrire	anomaly-detector*		
UpdateLogDelivery [autorisation uniquement]	Accorde l'autorisation de mettre à jour les informations de livraison de journaux pour la livraison de journaux spécifiée	Écrire			
UpdateLookupTable	Autorise la mise à jour d'une table de recherche	Écrire	lookup-table*		
UpdateScheduledQuery	Autorise la mise à jour d'une requête planifiée	Écrire	scheduled-query*		

Types de ressources définis par Amazon CloudWatch Logs

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
log-group	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
log-stream	arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}	aws:ResourceTag/${TagKey}
destination	arn:${Partition}:logs:${Region}:${Account}:destination:${DestinationName}	aws:ResourceTag/${TagKey}
delivery-source	arn:${Partition}:logs:${Region}:${Account}:delivery-source:${DeliverySourceName}	aws:ResourceTag/${TagKey}
delivery	arn:${Partition}:logs:${Region}:${Account}:delivery:${DeliveryName}	aws:ResourceTag/${TagKey}
delivery-destination	arn:${Partition}:logs:${Region}:${Account}:delivery-destination:${DeliveryDestinationName}	aws:ResourceTag/${TagKey}
anomaly-detector	arn:${Partition}:logs:${Region}:${Account}:anomaly-detector:${DetectorId}	aws:ResourceTag/${TagKey}
scheduled-query	arn:${Partition}:logs:${Region}:${Account}:scheduled-query:${ScheduledQueryId}	aws:ResourceTag/${TagKey}
lookup-table	arn:${Partition}:logs:${Region}:${Account}:lookup-table:${LookupTableName}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch Logs

Amazon CloudWatch Logs définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
logs:DeliveryDestinationResourceArn	Filtre l'accès en par l'ARN de destination Log Destination transmis dans la requête	ARN
logs:LogGenerating ResourceArns	Filtre l'accès par la ressource génératrice de journaux ARNs transmise dans la demande	ArrayOfARN

Actions, ressources et clés de condition pour Amazon CloudWatch Network Synthetic Monitor

Amazon CloudWatch Network Synthetic Monitor (préfixe de service :`networkmonitor`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Network Synthetic Monitor
- Types de ressources définis par Amazon CloudWatch Network Synthetic Monitor
- Clés de condition pour Amazon CloudWatch Network Synthetic Monitor

Actions définies par Amazon CloudWatch Network Synthetic Monitor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMonitor	Accorde la permission de créer un moniteur	Écrire	monitor*		
CreateProbe	Accorde l'autorisation de créer une sonde	Écrire			
DeleteMonitor	Accorde la permission de supprimer un moniteur	Écrire	monitor*		
DeleteProbe	Accorde l'autorisation de supprimer une sonde	Écrire	probe*		
GetMonitor	Accorde l'autorisation d'obtenir des informations sur un moniteur	Lecture	monitor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProbe	Accorde l'autorisation d'obtenir des informations sur une sonde	Lecture	probe*		
ListMonitors	Accorde l'autorisation de répertorier tous les moniteurs d'un compte et leurs statuts	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	monitor		
			probe		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource.	Balisage	monitor		
			probe		
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	monitor		
			probe		
				aws:TagKeys	
UpdateMonitor	Accorde l'autorisation de mettre à jour un moniteur	Écrire	monitor*		
UpdateProbe	Accorde l'autorisation de mettre à jour une sonde	Écrire	probe*		

Types de ressources définis par Amazon CloudWatch Network Synthetic Monitor

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
monitor	`arn:${Partition}:networkmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
probe	`arn:${Partition}:networkmonitor:${Region}:${Account}:probe/${ProbeId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch Network Synthetic Monitor

Amazon CloudWatch Network Synthetic Monitor définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtrer l'accès en fonction des clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access Manager (préfixe de service :oam) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Observability Access Manager
- Types de ressources définis par Amazon CloudWatch Observability Access Manager
- Clés de condition pour Amazon CloudWatch Observability Access Manager

Actions définies par Amazon CloudWatch Observability Access Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLink	Accorde l'autorisation de créer un lien entre un compte de surveillance et un compte source pour la surveillance entre comptes	Écrire	Sink*		oam:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys oam:ResourceTypes	
CreateSink	Accorde l'autorisation de créer un récepteur dans un compte afin qu'il puisse être utilisé comme compte de surveillance pour la surveillance entre comptes	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	Accorde l'autorisation de supprimer un lien entre un compte de surveillance et un compte source pour la surveillance entre comptes	Écrire	Link*		
				aws:ResourceTag/${TagKey}	
DeleteSink	Accorde l'autorisation de supprimer un récepteur de surveillance entre comptes dans un compte de surveillance	Écrire	Sink*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLink	Accorde l'autorisation de récupérer des informations complètes sur un lien de surveillance entre comptes	Lecture	Link*		
				aws:ResourceTag/${TagKey}	
GetSink	Accorde l'autorisation de récupérer des informations complètes sur un récepteur de surveillance entre comptes	Lecture	Sink*		
				aws:ResourceTag/${TagKey}	
GetSinkPolicy	Accorde l'autorisation de récupérer des informations sur la politique IAM pour un récepteur de surveillance entre comptes	Lecture	Sink*		
				aws:ResourceTag/${TagKey}	
ListAttachedLinks	Accorde l'autorisation de récupérer une liste de liens liés à un récepteur de surveillance entre comptes	Lecture	Sink*		
				aws:ResourceTag/${TagKey}	
ListLinks	Accorde l'autorisation de récupérer les liens ARNs de surveillance entre comptes de ce compte	Lecture			
ListSinks	Autorise la récupération des puits ARNs de surveillance entre comptes de ce compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	Link		
			Sink		
PutSinkPolicy	Accorde l'autorisation de créer ou mettre à jour la politique IAM pour un récepteur de surveillance entre comptes	Écrire	Sink*		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	Link		
			Sink		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	Link		
			Sink		
				aws:TagKeys	
UpdateLink	Accorde l'autorisation de mettre à jour un lien existant entre un compte de surveillance et un compte source	Écrire	Link*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} oam:ResourceTypes	

Types de ressources définis par Amazon CloudWatch Observability Access Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Link	`arn:${Partition}:oam:${Region}:${Account}:link/${ResourceId}`	aws:ResourceTag/${TagKey}
Sink	`arn:${Partition}:oam:${Region}:${Account}:sink/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés

pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
oam:ResourceTypes	Filtre l'accès en fonction de la présence de type de ressource dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch Observability Admin Service

Amazon CloudWatch Observability Admin Service (préfixe de service :`observabilityadmin`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Observability Admin Service

- Types de ressources définis par Amazon CloudWatch Observability Admin Service
- Clés de condition pour Amazon CloudWatch Observability Admin Service

Actions définies par Amazon CloudWatch Observability Admin Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCentralizationRuleForOrganization	Accorde l'autorisation de créer une nouvelle règle de centralisation d'organisation portant le nom spécifié pour l'organisation	Écrire	organization-centralization-rule*		
				aws:TagKeys aws:RequestTag/${TagKey} observabilityadmin:CentralizationSourceRegions observabilityadmin	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				:CentralizationDestinationRegion observabilityadmin:CentralizationBackupRegion	
CreateS3TableIntegration	Accorde l'autorisation de créer une nouvelle intégration de table s3 avec la configuration spécifiée	Écrire	s3tableintegration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTelemetryPipeline	Accorde l'autorisation de créer un nouveau pipeline de télémétrie avec le nom et la configuration spécifiés	Écrire	telemetry-pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} observabilityadmin:SourceType	
CreateTelemetryRule	Autorise la création d'une nouvelle règle de télémétrie portant le nom spécifié pour le compte	Écrire	telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTelemetryRuleForOrganization	Accorde l'autorisation de créer une nouvelle règle de télémétrie d'organisation portant le nom spécifié pour l'organisation	Écrire	organization-telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCentralizationRuleForOrganization	Accorde l'autorisation de supprimer une règle de centralisation d'organisation portant le nom spécifié pour l'organisation	Écrire	organization-centralization-rule*		
DeleteS3TableIntegration	Accorde l'autorisation de supprimer l'intégration de la table s3 avec l'arn spécifié	Écrire	s3tableintegration*		
DeleteTelemetryPipeline	Accorde l'autorisation de supprimer le pipeline de télémétrie avec l'arn spécifié	Écrire	telemetry-pipeline*		
DeleteTelemetryRule	Autorise la suppression d'une règle de télémétrie portant le nom spécifié pour le compte	Écrire	telemetry-rule*		
DeleteTelemetryRuleForOrganization	Accorde l'autorisation de supprimer une règle de télémétrie d'organisation portant le nom spécifié pour l'organisation	Écrire	organization-telemetry-rule*		
GetCentralizationRuleForOrganization	Accorde l'autorisation de récupérer la règle de centralisation d'organisation spécifiée pour l'organisation	Lecture	organization-centralization-rule*		
GetS3TableIntegration	Accorde l'autorisation de récupérer l'intégration de table s3 spécifiée pour le compte	Lecture	s3tableintegration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTelemetryEnrichmentStatus	Accorde l'autorisation de récupérer l'état des balises de ressource pour la fonctionnalité de télémétrie du compte	Lecture			
GetTelemetryEvaluationStatus	Accorde l'autorisation de récupérer l'état de la fonctionnalité Telemetry Config pour le compte	Lecture			
GetTelemetryEvaluationStatusForOrganization	Accorde l'autorisation de récupérer le statut de la fonctionnalité Telemetry Config pour l'organisation	Lecture			
GetTelemetryPipeline	Accorde l'autorisation d'obtenir le pipeline de télémétrie avec le nom ou l'ARN spécifié	Lecture	telemetry-pipeline*		
GetTelemetryRule	Accorde l'autorisation de récupérer la règle de télémétrie spécifiée pour le compte	Lecture	telemetry-rule*		
GetTelemetryRuleForOrganization	Accorde l'autorisation de récupérer la règle de télémétrie spécifiée pour l'organisation	Lecture	organization-telemetry-rule*		
ListCentralizationRulesForOrganization	Accorde l'autorisation de répertorier les règles de centralisation pour l'organisation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceTelemetry	Accorde l'autorisation de récupérer les configurations de télémétrie pour les ressources associées au compte	Lecture			
ListResourceTelemetryForOrganization	Accorde l'autorisation de récupérer les configurations de télémétrie pour les ressources associées aux comptes de l'organisation	Lecture			
ListS3TableIntegrations	Accorde l'autorisation de répertorier les intégrations de tables s3 pour le compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée	List	organization-centralization-rule		
			organization-telemetry-rule		
			s3tableintegration		
			telemetry-pipeline		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			telemetry-rule		
ListTelemetryPipelines	Autorise le compte à répertorier les pipelines de télémétrie	List			
ListTelemetryRules	Accorde l'autorisation de répertorier les règles de télémétrie pour le compte	List			
ListTelemetryRulesForOrganization	Autorise l'organisation à répertorier les règles de télémétrie	List			
StartTelemetryEnrichment	Accorde l'autorisation d'activer les balises de ressource pour la fonctionnalité de télémétrie pour le compte	Écrire			
StartTelemetryEvaluation	Autorise le lancement de la fonctionnalité de configuration de télémétrie pour le compte	Écrire			
StartTelemetryEvaluationForOrganization	Accorde l'autorisation de démarrer la fonctionnalité de configuration de télémétrie pour l'organisation	Écrire			
StopTelemetryEnrichment	Autorise le compte à désactiver les balises de ressource pour la fonctionnalité de télémétrie	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopTelemetryEvaluation	Accorde l'autorisation d'arrêter la fonctionnalité de configuration de télémétrie pour le compte	Écrire			
StopTelemetryEvaluationForOrganization	Autorise l'organisation à arrêter la fonctionnalité de configuration de télémétrie	Écrire			
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour les balises spécifiées pour la ressource spécifiée	Identification	organization-centralization-rule		
			organization-telemetry-rule		
			s3tableintegration		
			telemetry-pipeline		
			telemetry-rule		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
TestTelemetryPipeline	Autorise le test d'une configuration de pipeline de télémétrie avec des exemples de données	Lecture			
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de la ressource spécifiée	Identification	organization-centralization-rule		
			organization-telemetry-rule		
			s3tableintegration		
			telemetry-pipeline		
			telemetry-rule		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCentralizationRuleForOrganization	Accorde l'autorisation de mettre à jour la règle de centralisation spécifiée pour l'organisation	Écrire	organization-centralization-rule*		
				observabilityadmin:CentralizationSourceRegions observabilityadmin:CentralizationDestinationRegion observabilityadmin:CentralizationBackupRegion	
UpdateTelemetryPipeline	Accorde l'autorisation de mettre à jour le pipeline de télémétrie avec l'arn spécifié	Écrire	telemetry-pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTelemetryRule	Accorde l'autorisation de mettre à jour la règle de télémétrie spécifiée pour le compte	Écrire	telemetry-rule*		
UpdateTelemetryRuleForOrganization	Accorde l'autorisation de mettre à jour la règle de télémétrie spécifiée pour l'organisation	Écrire	organization-telemetry-rule*		
ValidateTelemetryPipelineConfiguration	Accorde l'autorisation de valider la configuration d'un pipeline de télémétrie	Lecture			

Types de ressources définis par Amazon CloudWatch Observability Admin Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
telemetry-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:telemetry-rule/${TelemetryRuleName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
organization-telemetry-rule	arn:${Partition}:observabilityadmin:${Region}:${Account}:organization-telemetry-rule/${TelemetryRuleName}	aws:ResourceTag/${TagKey}
organization-centralization-rule	arn:${Partition}:observabilityadmin:${Region}:${Account}:organization-centralization-rule/${CentralizationRuleName}	aws:ResourceTag/${TagKey}
telemetry-pipeline	arn:${Partition}:observabilityadmin:${Region}:${Account}:telemetry-pipeline/${TelemetryPipelineIdentifier}	aws:ResourceTag/${TagKey}
s3tableintegration	arn:${Partition}:observabilityadmin:${Region}:${Account}:s3tableintegration/${S3TableIntegrationIdentifier}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch Observability Admin Service

Amazon CloudWatch Observability Admin Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
observabilityadmin:CentralizationBackupRegion	Filtre l'accès en fonction de la région de sauvegarde transmise dans la demande	String
observabilityadmin:CentralizationDestinationRegion	Filtre l'accès en fonction de la région de destination transmise dans la demande	String
observabilityadmin:CentralizationSourceRegions	Filtre l'accès en fonction des régions sources transmises dans la demande	ArrayOfString
observabilityadmin:SourceType	Filtre l'accès en fonction du type de source transmis dans la demande	String

Actions, ressources et clés de condition pour AWS CloudWatch RUM

AWS CloudWatch RUM (préfixe de service :`rum`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CloudWatch RUM
- Types de ressources définis par AWS CloudWatch RUM
- Clés de condition pour AWS CloudWatch RUM

Actions définies par AWS CloudWatch RUM

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchCreateRumMetricDefinitions	Accorde l'autorisation de créer des définitions de métriques rum	Écrire	AppMonitorResource*		
BatchDeleteRumMetricDefinitions	Accorde l'autorisation de supprimer des définitions de métriques rum	Écrire	AppMonitorResource*		
BatchGetRumMetricDefinitions	Accorde l'autorisation d'obtenir des définitions de métriques rum	Lecture	AppMonitorResource*		
CreateAppMonitor	Accorde l'autorisation de créer des métadonnées appMonitor	Écrire	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppMonitor	Accorde l'autorisation de supprimer des métadonnées appMonitor	Écrire	AppMonitorResource*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressources attachée à un moniteur d'application	Écrire	AppMonitorResource*		
DeleteRumMetricsDestination	Accorde l'autorisation de supprimer des destinations de métriques rum	Écrire	AppMonitorResource*		
GetAppMonitor	Accorde l'autorisation d'obtenir des métadonnées appMonitor	Lecture	AppMonitorResource*		
GetAppMonitorData	Accorde l'autorisation d'obtenir des données appMonitor	Lecture	AppMonitorResource*		
GetResourcePolicy	Accorde l'autorisation de récupérer une politique de ressources attachée à un moniteur d'application	Lecture	AppMonitorResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAppMonitors	Accorde l'autorisation de répertorier des métadonnées appMonitor	List			
ListRumMetricsDestinations	Accorde l'autorisation de répertorier des destinations de métriques rum	Lecture	AppMonitorResource*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises des ressources	Lecture			
PutResourcePolicy	Accorde l'autorisation d'associer une politique de ressources à un moniteur d'application	Écrire	AppMonitorResource*		
PutRumEvents	Accorde l'autorisation de placer des événements RUM pour appMonitor	Écrire	AppMonitorResource*		
PutRumMetricsDestination	Accorde l'autorisation d'insérer des destinations de métriques rum	Écrire	AppMonitorResource*		
TagResource	Accorde l'autorisation de baliser des ressources	Identification	AppMonitorResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage des ressources	Identification	AppMonitorResource*		
				aws:TagKeys	
UpdateAppMonitor	Accorde l'autorisation de mettre à jour des métadonnées appMonitor	Écrire	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
UpdateRumMetricDefinition	Accorde l'autorisation de mettre à jour une définition de métriques rum	Écrire	AppMonitorResource*		

Types de ressources définis par AWS CloudWatch RUM

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AppMonitorResource	`arn:${Partition}:rum:${Region}:${Account}:appmonitor/${Name}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS CloudWatch RUM

AWS CloudWatch RUM définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande pour le compte du principal IAM	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource qui effectue la demande pour le compte du principal IAM	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande pour le compte du principal IAM	ArrayOfString

Actions, ressources et clés de condition pour Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics (préfixe de service `synthetics` :) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CloudWatch Synthetics
- Types de ressources définis par Amazon CloudWatch Synthetics
- Clés de condition pour Amazon CloudWatch Synthetics

Actions définies par Amazon CloudWatch Synthetics

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateResource	Accorde l'autorisation d'associer une ressource à un groupe	Écrire	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCanary	Accorde l'autorisation de créer un Canary.	Écrire		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateGroup	Accorde l'autorisation de créer un groupe.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCanary	Accorde l'autorisation de supprimer un Canary. Amazon Synthetics supprime toutes les ressources à l'exception de la fonction Lambda et des alarmes si vous en avez créé une. CloudWatch	Écrire	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteGroup	Accorde l'autorisation de supprimer un groupe	Écrire	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	Accorde l'autorisation de répertorier les informations de tous les Canary	Lecture		synthetics:Names	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCanariesLastRun	Accorde l'autorisation de répertorier des informations sur la dernière exécution de test associée à tous les Canary	Lecture		synthetics:Names	
DescribeRuntimeVersions	Autorise la création de la liste des informations sur les versions d'exécution de Canary Synthetics.	Lecture			
DisassociateResource	Accorde l'autorisation de dissocier une ressource d'un groupe	Écrire	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanary	Accorde l'autorisation d'afficher les informations d'un Canary	Lecture	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanaryRuns	Accorde l'autorisation de répertorier des informations sur toutes les exécutions de tests associées à un Canary	Lecture	canary*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	Accorde l'autorisation d'afficher les informations d'un groupe	Lecture	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListAssociatedGroups	Accorde l'autorisation de répertorier des informations relatives aux groupes associés d'un Canary	List	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources	Accorde l'autorisation de répertorier des informations relatives au canarys dans un groupe	List	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGroups	Accorde l'autorisation de répertorier les informations de tous les groupes	List			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les identifications et valeurs associées à une ressource	Lecture	canary		
			group		
StartCanary	Accorde l'autorisation de créer un canari, afin qu'Amazon CloudWatch Synthetics commence à surveiller un site Web	Écrire	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StartCanaryDryRun	Autorise le lancement d'un Canary Dry Run, afin qu'Amazon CloudWatch Synthetics puisse exécuter un test d'exécution d'un Canary avec les paramètres fournis	Écrire	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StopCanary	Accorde l'autorisation d'arrêter un Canary	Écrire	canary*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une ressource	Balisage	canary		
			group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Identification	canary		
			group		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	Accorde l'autorisation de mettre à jour un Canary	Écrire	canary*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	

Types de ressources définis par Amazon CloudWatch Synthetics

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
canary	`arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}`	aws:ResourceTag/${TagKey}
group	`arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics définit les clés de condition suivantes qui peuvent être utilisées dans `Condition` l'élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString
synthetics:Names	Filtre l'accès en fonction du nom du Canary	ArrayOfString

Actions, ressources et clés de condition pour AWS CodeArtifact

AWS CodeArtifact (préfixe de service :`codeartifact`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CodeArtifact
- Types de ressources définis par AWS CodeArtifact
- Clés de condition pour AWS CodeArtifact

Actions définies par AWS CodeArtifact

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateExternalConnection	Accorde l'autorisation d'ajouter une connexion externe à un référentiel	Écriture	repository*		
AssociateWithDownstreamRepository	Accorde l'autorisation d'associer un référentiel existant en tant que référentiel en amont à un autre référentiel	Écrire	repository*		
CopyPackageVersions	Accorde l'autorisation de copier des versions de package d'un référentiel vers un autre référentiel dans le même domaine	Écrire	package* repository*		
CreateDomain	Accorde l'autorisation de créer un domaine	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackageGroup	Accorde l'autorisation de créer un groupe de packages	Écrire		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateRepository	Accorde l'autorisation de créer un référentiel	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDomain	Accorde l'autorisation de supprimer un domaine	Écriture	domain*		
DeleteDomainPermissionsPolicy	Accorde l'autorisation de supprimer la politique de ressource définie sur un domaine	Gestion des autorisations	domain*		
DeletePackage	Accorde l'autorisation de supprimer un package	Écrire	package*		
DeletePackageGroup	Accorde l'autorisation de supprimer un groupe de packages	Écrire	package-group*		
DeletePackageVersions	Accorde l'autorisation de supprimer des versions de package	Écriture	package*		
DeleteRepository	Accorde l'autorisation de supprimer un référentiel	Écriture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRepositoryPermissionsPolicy	Accorde l'autorisation de supprimer la politique de ressource définie pour un référentiel	Gestion des autorisations	repository*		
DescribeDomain	Accorde l'autorisation de renvoyer des informations sur un domaine	Lecture	domain*		
DescribePackage	Accorde l'autorisation de récupérer des informations sur un package	Lecture	package*		
DescribePackageGroup	Accorde l'autorisation de renvoyer des informations détaillées sur un groupe de packages	Lecture	package-group*		
DescribePackageVersion	Accorde l'autorisation de renvoyer des informations sur une version de package	Lecture	package*		
DescribeRepository	Accorde l'autorisation de renvoyer des informations détaillées sur un référentiel	Lecture	repository*		
DisassociateExternalConnection	Accorde l'autorisation de dissocier une connexion externe d'un référentiel	Écriture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisposePackageVersions	Accorde l'autorisation de définir l'état des versions de package sur Disposed et de supprimer leurs ressources	Écrire	package*		
GetAssociatedPackageGroup	Accorde l'autorisation de renvoyer le groupe de colis associé à un package	Lecture	package-group*		
GetAuthorizationToken	Accorde l'autorisation de générer un jeton d'authentification temporaire pour accéder aux référentiels d'un domaine	Lecture	domain*		
GetDomainPermissionsPolicy	Accorde l'autorisation de renvoyer la politique de ressource d'un domaine	Lecture	domain*		
GetPackageVersionAsset	Accorde l'autorisation de renvoyer une ressource (ou un fichier) faisant partie d'une version de package	Lecture	package*		
GetPackageVersionReadme	Accorde l'autorisation de renvoyer le fichier readme d'une version de package	Lecture	package*		
GetRepositoryEndpoint	Accorde l'autorisation de renvoyer un point de terminaison pour un référentiel	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRepositoryPermissionsPolicy	Accorde l'autorisation de renvoyer la politique de ressource d'un référentiel	Lecture	repository*		
ListAllowedRepositoriesForGroup	Accorde l'autorisation de répertorier les référentiels autorisés pour un groupe de packages	List	package-group*		
ListAssociatedPackages	Accorde l'autorisation de répertorier les packages associés à un groupe de packages	List	package-group*		
ListDomains	Accorde l'autorisation de répertorier les domaines de l'utilisateur actuel Compte AWS	List			
ListPackageGroups	Accorde l'autorisation de répertorier les groupes de packages dans un domaine	List	domain*		
ListPackageVersionAssets	Accorde l'autorisation de répertorier les ressources d'une version de package	Liste	package*		
ListPackageVersionDependencies	Accorde l'autorisation de répertorier les dépendances directes d'une version de package	Liste	package*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPackageVersions	Accorde l'autorisation de répertorier les versions d'un package	Liste	package*		
ListPackages	Accorde l'autorisation de répertorier les packages dans un référentiel	Liste	repository*		
ListRepositories	Accorde l'autorisation de répertorier les référentiels administrés par le compte appelant	Liste			
ListRepositoriesInDomain	Accorde l'autorisation de répertorier les référentiels dans un domaine	List	domain*		
ListSubPackageGroups	Accorde l'autorisation de répertorier les sous-groupes de packages pour un groupe de packages parent	List	package-group*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une CodeArtifact ressource	List	domain		
			package-group		
			repository		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PublishPackageVersion	Accorde l'autorisation de publier des ressources et des métadonnées au niveau du point de terminaison d'un référentiel	Écriture	package*		
PutDomainPermissionsPolicy	Accorde l'autorisation d'attacher une politique de ressource à un domaine	Écriture	domain*		
PutPackageMetadata	Accorde l'autorisation d'ajouter, de modifier ou de supprimer des métadonnées de package à l'aide d'un point de terminaison de référentiel	Écrire	package*		
PutPackageOriginConfiguration	Accorde l'autorisation de définir la configuration d'origine d'un package	Écrire	package*		
PutRepositoryPermissionsPolicy	Accorde l'autorisation d'attacher une politique de ressource à un référentiel	Écriture	repository*		
ReadFromRepository	Accorde l'autorisation de renvoyer des ressources et des métadonnées de package à partir d'un point de terminaison de référentiel	Lecture	repository*		
TagResource		Identification	domain		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de baliser une CodeArtifact ressource		package-group		
			repository		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer un tag d'une CodeArtifact ressource	Identification	domain		
			package-group		
			repository		
				aws:TagKeys	
UpdatePackageGroup	Accorde l'autorisation de modifier les propriétés d'un groupe de packages	Écrire	package-group*		
UpdatePackageGroupOriginConfiguration	Accorde l'autorisation de modifier la configuration d'origine du package d'un groupe de packages	Écrire	package-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePackageVersionsStatus	Accorde l'autorisation de modifier l'état d'une ou de plusieurs versions d'un package	Écriture	package*		
UpdateRepository	Accorde l'autorisation de modifier les propriétés d'un référentiel	Écrire	repository*		

Types de ressources définis par AWS CodeArtifact

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> L'ARN de la ressource de groupes de packages doit utiliser un modèle de groupe de packages codé.

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:codeartifact:${Region}:${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
repository	`arn:${Partition}:codeartifact:${Region}:${Account}:repository/${DomainName}/${RepositoryName}`	aws:ResourceTag/${TagKey}
package-group	`arn:${Partition}:codeartifact:${Region}:${Account}:package-group/${DomainName}${EncodedPackageGroupPattern}`	aws:ResourceTag/${TagKey}
package	`arn:${Partition}:codeartifact:${Region}:${Account}:package/${DomainName}/${RepositoryName}/${PackageFormat}/${PackageNamespace}/${PackageName}`	

Clés de condition pour AWS CodeArtifact

AWS CodeArtifact définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CodeCatalyst

Amazon CodeCatalyst (préfixe de service :`codecatalyst`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CodeCatalyst
- Types de ressources définis par Amazon CodeCatalyst
- Clés de condition pour Amazon CodeCatalyst

Actions définies par Amazon CodeCatalyst

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptConnection [autorisation uniquement]	Accorde l'autorisation d'accepter une demande de connexion de ce compte à un CodeCatalyst espace Amazon	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateIamRoleToConnection [autorisation uniquement]	Accorde l'autorisation d'associer une connexion à un rôle IAM	Écrire	connections*		iam:PassRole
				aws:ResourceTag/${TagKey}	
AssociateIdentityCenterApplicationToSpace [autorisation uniquement]	Accorde l'autorisation d'associer une application IAM Identity Center à un espace Amazon CodeCatalyst	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
AssociateIdentityToIdentityCenterApplication [autorisation uniquement]	Accorde l'autorisation d'associer une identité à une application IAM Identity Center pour un espace Amazon CodeCatalyst	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchAssociateIdentitiesToIdentityCenterApplication [autorisation uniquement]	Accorde l'autorisation d'associer plusieurs identités à une application IAM Identity Center pour un espace Amazon CodeCatalyst	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateIdentitiesFromIdentityCenterApplication [autorisation uniquement]	Accorde l'autorisation de dissocier plusieurs identités d'une application IAM Identity Center pour un espace Amazon CodeCatalyst	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
CreateIdentityCenterApplication [autorisation uniquement]	Octroie l'autorisation de créer une application IAM Identity Center.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSpace [autorisation uniquement]	Accorde l'autorisation de créer un CodeCatalyst espace Amazon	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSpaceAdminRoleAssignment [autorisation uniquement]	Accorde l'autorisation de créer une attribution de rôle d'administrateur pour un CodeCatalyst espace Amazon donné et une application IAM Identity Center	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DeleteConnection [autorisation uniquement]	Accorde l'autorisation de supprimer une connexion.	Écrire	connections*		
				aws:ResourceTag/${TagKey}	
DeleteIdentityCenterApplication [autorisation uniquement]	Octroie l'autorisation de supprimer une application IAM Identity Center.	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIamRoleFromConnection [autorisation uniquement]	Accorde l'autorisation de dissocier un rôle IAM d'une connexion	Écrire	connections*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateIdentityCenterApplicationFromSpace [autorisation uniquement]	Accorde l'autorisation de dissocier une application IAM Identity Center d'un espace Amazon CodeCatalyst	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityFromIdentityCenterApplication [autorisation uniquement]	Accorde l'autorisation de dissocier une identité d'une application IAM Identity Center pour un espace Amazon CodeCatalyst	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetBillingAuthorization [autorisation uniquement]	Accorde l'autorisation de décrire l'autorisation de facturation pour une connexion	Lecture	connections*		
				aws:ResourceTag/${TagKey}	
GetConnection [autorisation uniquement]	Accorde l'autorisation d'obtenir une connexion	Lecture	connections*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetIdentityCenterApplication [autorisation uniquement]	Octroie l'autorisation d'obtenir des informations sur une application IAM Identity Center.	Lecture	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
GetPendingConnection [autorisation uniquement]	Accorde l'autorisation de recevoir une demande en attente pour connecter ce compte à un CodeCatalyst espace Amazon	Lecture			
ListConnections [autorisation uniquement]	Accorde l'autorisation de répertorier les connexions qui ne sont pas en attente	List			
ListIamRolesForConnection [autorisation uniquement]	Accorde l'autorisation d'énumérer les rôles IAM associé à une connexion	List	connections*		
				aws:ResourceTag/${TagKey}	
ListIdentityCenterApplications [autorisation uniquement]	Octroie l'autorisation d'afficher une liste de toutes les applications IAM Identity Center du compte.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIdentityCenterApplicationsForSpace [autorisation uniquement]	Autorise Amazon CodeCatalyst Space à consulter la liste des applications IAM Identity Center	List			
ListSpacesForIdentityCenterApplication [autorisation uniquement]	Autorise l'accès à la liste des CodeCatalyst espaces Amazon par application IAM Identity Center	List	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation de répertorier les tags d'une CodeCatalyst ressource Amazon	Lecture	connections		
			identity-center-applications		
				aws:ResourceTag/${TagKey}	
PutBillingAuthorization [autorisation uniquement]	Accorde l'autorisation de créer ou de mettre à jour l'autorisation de facturation pour une connexion	Écrire	connections*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
RejectConnection [autorisation uniquement]	Autorise le rejet d'une demande de connexion de ce compte à un CodeCatalyst espace Amazon	Écrire			
SynchronizeIdentityCenterApplication [autorisation uniquement]	Octroie l'autorisation de synchroniser une application IAM Identity Center avec le magasin d'identités sous-jacent.	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
TagResource [autorisation uniquement]	Accorde l'autorisation de baliser une CodeCatalyst ressource Amazon	Identification	connections		
			identity-center-applications		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation de supprimer le balisage d'une ressource Amazon CodeCatalyst	Identification	connections		
			identity-center-applications		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateIdentityCenterApplication [autorisation uniquement]	Octroie l'autorisation de mettre à jour une application IAM Identity Center.	Écrire	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon CodeCatalyst

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
connections	`arn:${Partition}:codecatalyst:${Region}:${Account}:/connections/${ConnectionId}`	aws:ResourceTag/${TagKey}
identity-center-applications	`arn:${Partition}:codecatalyst:${Region}:${Account}:/identity-center-applications/${IdentityCenterApplicationId}`	aws:ResourceTag/${TagKey}
space	`arn:${Partition}:codecatalyst:::space/${SpaceId}`	
project	`arn:${Partition}:codecatalyst:::space/${SpaceId}/project/${ProjectId}`	

Clés de condition pour Amazon CodeCatalyst

Amazon CodeCatalyst définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString

Actions, ressources et clés de condition pour AWS CodeCommit

AWS CodeCommit (préfixe de service :`codecommit`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CodeCommit
- Types de ressources définis par AWS CodeCommit
- Clés de condition pour AWS CodeCommit

Actions définies par AWS CodeCommit

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateApprovalRuleTemplateWithRepository	Accorde l'autorisation d'associer un modèle de règle d'approbation à un référentiel	Écriture	repository*		
BatchAssociateApprovalRuleTemplateWithRepositories	Accorde l'autorisation d'associer un modèle de règle d'approbation à plusieurs référentiels en une seule opération	Écriture	repository*		
BatchDescribeMergeConflicts	Accorde l'autorisation d'obtenir des informations sur plusieurs conflits de fusion lors de la tentative de fusionner deux validations à l'aide de l'option de fusion par triangulation ou de l'option de fusion par écrasement	Lecture	repository*		
BatchDisassociateApprovalRuleTemplateFromRepositories	Accorde l'autorisation de supprimer l'association entre un modèle de règle d'approbation et plusieurs référentiels en une seule opération	Écrire	repository*		
BatchGetCommits	Accorde l'autorisation de renvoyer des informations sur	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	un ou plusieurs validations dans un AWS CodeCommit référentiel				
BatchGetPullRequests [autorisation uniquement]	Accorde l'autorisation de renvoyer des informations sur une ou plusieurs pull requests dans un AWS CodeCommit référentiel	Lecture	repository*		
BatchGetRepositories	Accorde l'autorisation d'obtenir des informations sur plusieurs référentiels	Lecture	repository*		
CancelUploadArchive [autorisation uniquement]	Accorde l'autorisation d'annuler le téléchargement d'une archive vers un pipeline dans AWS CodePipeline	Lecture	repository*		
CreateApprovalRuleTemplate	Accorde l'autorisation de créer un modèle de règle d'approbation qui crée automatiquement les règles d'approbation dans les demandes d'extraction correspondant aux conditions définies dans le modèle ; n'accorde pas l'autorisation de créer des règles d'approbation pour les demandes d'extraction individuelles.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBranch	Accorde l'autorisation de créer une branche dans un AWS CodeCommit dépôt avec cette API ; ne contrôle pas les actions de création de branche de Git	Écrire	repository*		
				codecommit:References	
CreateCommit	Accorde l'autorisation d'ajouter, de copier, de déplacer ou de mettre à jour un ou plusieurs fichiers dans une branche d'un AWS CodeCommit référentiel, et de générer un commit pour les modifications dans la branche spécifiée	Écrire	repository*		
				codecommit:References	
CreatePullRequest	Accorde l'autorisation de créer une demande d'extraction dans le référentiel spécifié	Écriture	repository*		
CreatePullRequestApprovalRule	Accorde l'autorisation de créer une règle d'approbation spécifique à une demande d'extraction individuelle ; n'accorde pas l'autorisation de créer des modèles de règle d'approbation	Écrire	repository*		
CreateRepository	Octroie l'autorisation de créer un AWS CodeCommit dépôt	Écrire	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUnreferencedMergeCommit	Accorde l'autorisation de créer une validation non référencée qui contient le résultat de la fusion de deux validations à l'aide de l'option de fusion par triangulation ou de l'option de fusion par écrasement ; ne contrôle pas les actions de fusion Git	Écriture	repository*		
				codecommit:References	
DeleteApprovalRuleTemplate	Accorde l'autorisation de supprimer un modèle de règle d'approbation	Écrire			
DeleteBranch	Accorde l'autorisation de supprimer une branche dans un AWS CodeCommit dépôt avec cette API ; ne contrôle pas les actions de suppression de branche par Git	Écrire	repository*		
				codecommit:References	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCommentContent	Accorde l'autorisation pour supprimer le contenu d'un commentaire effectué sur une modification, un fichier ou une validation dans un référentiel	Écriture	repository*		
DeleteFile	Accorde l'autorisation de supprimer un fichier spécifié à partir d'une branche spécifiée	Écriture	repository*		
				codecommit:References	
DeletePullRequestApprovalRule	Accorde l'autorisation de supprimer une règle d'approbation créée pour une demande d'extraction si la règle n'a pas été créée par un modèle de règle d'approbation	Écrire	repository*		
DeleteRepository	Accorde l'autorisation de supprimer un AWS CodeCommit dépôt	Écrire	repository*		
DescribeMergeConflicts	Accorde l'autorisation d'obtenir des informations sur des conflits de fusion spécifiques lors de la tentative de fusionner deux validations à l'aide de l'option de fusion par triangulation ou de l'option de fusion par écrasement	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribePullRequestEvents	Accorde l'autorisation de renvoyer des informations sur un ou plusieurs événements de demande d'extraction.	Lecture	repository*		
DisassociateApprovalRuleTemplateFromRepository	Accorde l'autorisation de supprimer l'association entre un modèle de règle d'approbation et un référentiel	Écriture	repository*		
EvaluatePullRequestApprovalRules	Accorde l'autorisation d'évaluer si une demande d'extraction peut être fusionnée en fonction de son état d'approbation actuel et des exigences de règle d'approbation	Lecture	repository*		
GetApprovalRuleTemplate	Accorde l'autorisation de retourner des informations sur un modèle de règle d'approbation	Lecture			
GetBlob	Autorise l'affichage du contenu codé d'un fichier individuel dans un AWS CodeCommit référentiel à partir de la AWS CodeCommit console	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBranch	Accorde l'autorisation d'obtenir des informations sur une branche d'un AWS CodeCommit dépôt avec cette API ; ne contrôle pas les actions de branche Git	Lecture	repository*		
GetComment	Accorde l'autorisation pour obtenir le contenu d'un commentaire effectué sur une modification, un fichier ou une validation dans un référentiel	Lecture	repository*		
GetCommentReactions	Accorde l'autorisation d'obtenir les réactions sur un commentaire	Lecture	repository*		
GetCommentsForComparedCommit	Accorde l'autorisation d'obtenir des informations sur des commentaires effectués sur la comparaison entre deux validations	Lecture	repository*		
GetCommentsForPullRequest	Accorde l'autorisation d'obtenir des commentaires effectués sur une demande d'extraction	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCommit	Accorde l'autorisation de renvoyer les informations sur une validation, y compris le message de validation et les informations sur le valideur, avec cette API ; ne contrôle pas les actions de journal Git	Lecture	repository*		
GetCommitHistory [autorisation uniquement]	Accorde l'autorisation d'obtenir des informations sur l'historique des validations d'un référentiel	Lecture	repository*		
GetCommitsFromMergeBase [autorisation uniquement]	Accorde l'autorisation d'obtenir des informations sur la différence entre les validations dans le contexte d'une fusion potentielle	Lecture	repository*		
GetDifferences	Accorde l'autorisation d'afficher les informations sur les différences entre les spécificateurs de validation valides (par exemple, branche, balise, HEAD, ID de validation ou autre référence complète)	Lecture	repository*		
GetFile	Accorde l'autorisation de renvoyer le contenu codé en base 64 d'un fichier spécifié et de ses métadonnées	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFolder	Accorde l'autorisation de renvoyer le contenu d'un dossier spécifié dans un référentiel	Lecture	repository*		
GetMergeCommit	Accorde l'autorisation d'obtenir des informations sur une validation de fusion créée par l'une des options de fusion des demandes d'extraction qui crée les validations de fusion. Certaines options de fusion ne créent pas de validations de fusion. Cette autorisation ne contrôle pas les actions de fusion Git	Lecture	repository*		
				codecommit:References	
GetMergeConflicts	Accorde l'autorisation d'obtenir des informations sur les conflits de fusion entre le commit avant et après IDs pour une pull request dans un référentiel	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMergeOptions	Accorde l'autorisation d'obtenir les informations sur les options de fusion pour les demandes d'extraction qui peuvent être utilisées pour fusionner deux validations ; ne contrôle pas les actions de fusion Git	Lecture	repository*		
GetObjectIdentifier [autorisation uniquement]	Accorde l'autorisation pour résoudre les objets BLOB, les arborescences et les validations par rapport à leur identifiant	Lecture	repository*		
GetPullRequest	Accorde l'autorisation d'obtenir des informations sur une demande d'extraction dans un référentiel spécifié	Lecture	repository*		
GetPullRequestApprovalStates	Accorde l'autorisation de récupérer les approbations actuelles sur une demande d'extraction en entrée	Lecture	repository*		
GetPullRequestOverrideState	Accorde l'autorisation de récupérer l'état de remplacement actuel d'une demande d'extraction donnée	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetReferences [autorisation uniquement]	Accorde l'autorisation d'obtenir des détails sur les références d'un AWS CodeCommit dépôt ; ne contrôle pas les actions de référence Git	Lecture	repository*		
GetRepository	Accorde l'autorisation d'obtenir des informations sur un AWS CodeCommit dépôt	Lecture	repository*		
GetRepositoryTriggers	Accorde l'autorisation d'obtenir des informations sur les déclencheurs configurés pour un référentiel	Lecture	repository*		
GetTree [autorisation uniquement]	Accorde l'autorisation d'afficher le contenu d'une arborescence spécifiée dans un AWS CodeCommit référentiel à partir de la AWS CodeCommit console	Lecture	repository*		
GetUploadArchiveStatus [autorisation uniquement]	Accorde l'autorisation d'obtenir des informations sur le statut d'un téléchargement d'archive vers un pipeline dans AWS CodePipeline	Lecture	repository*		
GitPull [autorisation uniquement]	Accorde l'autorisation d'extraire des informations d'un AWS CodeCommit référentiel vers un dépôt local	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GitPush [autorisation uniquement]	Accorde l'autorisation de transférer des informations d'un dépôt local vers un AWS CodeCommit référentiel	Écrire	repository*		
				codecommit:References	
ListApprovalRuleTemplates	Accorde l'autorisation de répertorier tous les modèles de règles d'approbation dans et Région AWS pour le Compte AWS	List			
ListAssociatedApprovalRuleTemplatesForRepository	Accorde l'autorisation de répertorier les modèles de règle d'approbation associés à un référentiel	List	repository*		
ListBranches	Accorde l'autorisation de répertorier les branches d'un AWS CodeCommit dépôt avec cette API ; ne contrôle pas les actions des branches Git	List	repository*		
ListFileCommitHistory	Accorde l'autorisation de répertorier les validations et les modifications apportées à un fichier spécifié	List	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPullRequests	Accorde l'autorisation de répertorier les demandes d'extraction d'un référentiel spécifié	List	repository*		
ListRepositories	Accorde l'autorisation de répertorier des informations sur AWS CodeCommit les référentiels de la région actuelle pour votre Compte AWS	List			
ListRepositoriesForApprovalRuleTemplate	Accorde l'autorisation de répertorier les référentiels associés à un modèle de règle d'approbation	List			
ListTagsForResource	Accorde l'autorisation de répertorier la ressource attachée à un ARN de CodeCommit ressource	List	repository		
MergeBranchesByFastForward	Accorde l'autorisation de fusionner deux validations dans la branche de destination spécifiée à l'aide de l'option de fusion rapide	Écriture	repository*		
				codecommit:References	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
MergeBranchesBySquash	Accorde l'autorisation de fusionner deux validations dans la branche de destination spécifiée à l'aide de l'option de fusion par écrasement	Écriture	repository*		
				codecommit:References	
MergeBranchesByThreeWay	Accorde l'autorisation de fusionner deux validations dans la branche de destination spécifiée à l'aide de l'option de fusion par triangulation	Écriture	repository*		
				codecommit:References	
MergePullRequestByFastForward	Accorde l'autorisation de fermer une demande d'extraction et de tenter de la fusionner dans la branche de destination spécifiée pour cette demande d'extraction à la validation spécifiée à l'aide de l'option de fusion rapide	Écriture	repository*		
				codecommit:References	
MergePullRequestBySquash	Accorde l'autorisation de fermer une demande d'extraction et de tenter de la fusionner dans la branche de destination spécifiée pour cette demande d'extraction à la validation spécifiée à l'aide de l'option de fusion par écrasement	Écriture	repository*		
				codecommit:References	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
MergePullRequestByThreeWay	Accorde l'autorisation de fermer une demande d'extraction et de tenter de la fusionner dans la branche de destination spécifiée pour cette demande d'extraction à la validation spécifiée à l'aide de l'option de fusion par triangulation	Écriture	repository*		
				codecommit:References	
OverridePullRequestApprovalRules	Accorde l'autorisation de remplacer toutes les règles d'approbation pour une demande d'extraction, y compris les règles d'approbation créées par un modèle	Écriture	repository*		
PostCommentForComparedCommit	Accorde l'autorisation de publier un commentaire sur la comparaison entre deux validations	Écriture	repository*		
PostCommentForPullRequest	Accorde l'autorisation de publier un commentaire sur une demande d'extraction	Écriture	repository*		
PostCommentReply	Accorde l'autorisation de publier un commentaire en réponse à un commentaire sur une comparaison entre des validations ou sur une demande d'extraction	Écriture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutCommentReaction	Accorde l'autorisation de publier une réaction sur un commentaire	Écrire	repository*		
PutFile	Accorde l'autorisation d'ajouter ou de mettre à jour un fichier dans une branche d'un AWS CodeCommit référentiel et de générer un commit pour l'ajout dans la branche spécifiée	Écrire	repository*		
				codecommit:References	
PutRepositoryTriggers	Accorde l'autorisation de créer, de mettre à jour ou de supprimer les déclencheurs d'un référentiel	Écrire	repository*		
TagResource	Accorde l'autorisation d'associer des balises de ressource à un ARN de CodeCommit ressource	Identification	repository		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestRepositoryTriggers	Accorde l'autorisation de tester la fonctionnalité des déclencheurs de référentiel en envoyant des informations à la cible du déclencheur	Écrire	repository*		
UntagResource	Accorde l'autorisation de dissocier les balises de ressources d'un ARN de CodeCommit ressource	Identification	repository		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApprovalRuleTemplateContent	Accorde l'autorisation de mettre à jour le contenu des modèles de règle d'approbation ; n'accorde pas l'autorisation de mettre à jour le contenu des règles d'approbation créées spécifiquement pour les demandes d'extraction	Écriture			
UpdateApprovalRuleTemplateDescription	Accorde l'autorisation de mettre à jour la description des modèles de règle d'approbation	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApprovalRuleTemplateName	Accorde l'autorisation de mettre à jour le nom des modèles de règle d'approbation	Écriture			
UpdateComment	Accorde l'autorisation de mettre à jour le contenu d'un commentaire si l'identité correspond à l'identité utilisée pour créer le commentaire	Écrire	repository*		
UpdateDefaultBranch	Accorde l'autorisation de modifier la branche par défaut dans un AWS CodeCommit référentiel	Écrire	repository*		
UpdatePullRequestApprovalRuleContent	Accorde l'autorisation de mettre à jour le contenu des règles d'approbation créées pour une demande d'extraction spécifique ; n'accorde pas l'autorisation de mettre à jour le contenu de la règle d'approbation pour les règles créées avec un modèle de règle d'approbation	Écriture	repository*		
UpdatePullRequestApprovalState	Accorde l'autorisation de mettre à jour l'état d'approbation pour les demandes d'extraction	Écriture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePullRequestDescription	Accorde l'autorisation de mettre à jour la description d'une demande d'extraction	Écriture	repository*		
UpdatePullRequestStatus	Accorde une autorisation de mettre à jour le statut d'une demande d'extraction	Écriture	repository*		
UpdatePullRequestTitle	Accorde l'autorisation de mettre à jour le titre d'une demande d'extraction	Écrire	repository*		
UpdateRepositoryDescription	Accorde l'autorisation de modifier la description d'un AWS CodeCommit dépôt	Écrire	repository*		
UpdateRepositoryEncryptionKey	Accorde l'autorisation de modifier la clé de chiffrement AWS KMS utilisée pour chiffrer et déchiffrer un référentiel AWS CodeCommit	Écrire	repository*		
UpdateRepositoryName	Accorde l'autorisation de modifier le nom d'un AWS CodeCommit dépôt	Écrire	repository*		
UploadArchive [autorisation uniquement]	Accorde au rôle de service l'autorisation AWS CodePipeline de télécharger les modifications du référentiel dans un pipeline	Écrire	repository*		

Types de ressources définis par AWS CodeCommit

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
repository	`arn:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS CodeCommit

AWS CodeCommit définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Clés de condition	Description	Type
codecommit:References	Filtre l'accès par référence Git aux AWS CodeCommit actions spécifiées	String

Actions, ressources et clés de condition pour AWS CodeConnections

AWS CodeConnections (préfixe de service :`codeconnections`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CodeConnections
- Types de ressources définis par AWS CodeConnections
- Clés de condition pour AWS CodeConnections

Actions définies par AWS CodeConnections

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConnection	Accorde l'autorisation de créer une ressource de connexion.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType	
CreateHost	Accorde l'autorisation de créer une ressource hôte	Écrire		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType codeconnections:VpcId	
CreateRepositoryLink	Octroie l'autorisation de créer un lien de référentiel.	Écrire	Connection*		codeconnections:PassConnection

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					codeconnections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Accorde l'autorisation de créer une config de synchronisation de modèle	Écrire	RepositoryLink*		codeconnections:PassRepository iam:PassRole
				codeconnections:Branch	
DeleteConnection	Accorde l'autorisation de supprimer une ressource de connexion.	Écriture	Connection*		
DeleteHost	Accorde l'autorisation de supprimer une ressource hôte.	Écrire	Host*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRepositoryLink	Octroie l'autorisation de supprimer un lien de référentiel.	Écrire	RepositoryLink*		
DeleteSyncConfiguration	Octroie l'autorisation de supprimer une configuration de synchronisation.	Écrire			
GetConnection	Accorde l'autorisation d'obtenir des détails sur une ressource de connexion	Lecture	Connection*		
GetConnectionToken [autorisation uniquement]	Accorde l'autorisation d'obtenir un jeton de connexion pour appeler les actions du fournisseur	Lecture	Connection*		
GetHost	Accorde l'autorisation d'obtenir des détails sur une ressource hôte.	Lecture	Host*		
GetIndividualAccessToken [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	Lecture		codeconnections:ProviderType	codeconnections:StartOAuthHandshake
GetInstallationUrl [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	Lecture		codeconnections:ProviderType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRepositoryLink	Octroie l'autorisation de décrire un lien de référentiel.	Lecture	RepositoryLink*		
GetRepositorySyncStatus	Accorde l'autorisation d'obtenir le dernier statut de synchronisation d'un référentiel	Lecture	RepositoryLink*		
				codeconnections:Branch	
GetResourceSyncStatus	Octroie l'autorisation d'obtenir le dernier statut de synchronisation d'une ressource (pile cfn ou autres ressources).	Lecture			
GetSyncBlockerSummary	Octroie l'autorisation de décrire les bloqueurs de synchronisation de service sur une ressource (pile cfn ou autres ressources).	Lecture			
GetSyncConfiguration	Octroie l'autorisation de décrire une configuration de synchronisation.	Lecture			
ListConnections	Accorde l'autorisation de répertorier les ressources de connexion	Liste	Connection*		
				codeconnections:ProviderTypeFilter	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListHosts	Accorde l'autorisation de répertorier des ressources hôtes	Liste		codeconnections:ProviderTypeFilter	
ListInstallationTargets [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	List			codeconnections:GetIndividualAccessToken codeconnections:StartOAuthHandshake
ListRepositoryLinks	Octroie l'autorisation de répertorier les liens de référentiels.	List			
ListRepositorySyncDefinitions	Accorde l'autorisation de répertorier les définitions de synchronisation de référentiel	List			
ListSyncConfigurations	Octroie l'autorisation de répertorier les configurations de synchronisation d'un lien de référentiel.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation d'obtenir l'ensemble des paires clé-valeur utilisées pour gérer la ressource	List	Connection		
			Host		
			RepositoryLink		
PassConnection [autorisation uniquement]	Accorde l'autorisation de transmettre une ressource de connexion à un AWS service qui accepte un ARN de connexion en entrée, tel que codepipeline : CreatePipeline	Lecture	Connection*		
				codeconnections:PassedToService	
PassRepository [autorisation uniquement]	Accorde l'autorisation de transmettre une ressource de lien de référentiel à un AWS service qui accepte un RepositoryLinkId comme entrée, tel que codeconnections : CreateSyncConfiguration	Lecture	RepositoryLink*		
				codeconnections:PassedToService	
RegisterAppCode [autorisation uniquement]	Accorde l'autorisation d'associer un serveur tiers, tel qu'une instance de serveur GitHub d'entreprise, à un hôte	Lecture		codeconnections:HostArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartAppRegistrationHandshake [autorisation uniquement]	Accorde l'autorisation d'associer un serveur tiers, tel qu'une instance de serveur GitHub d'entreprise, à un hôte	Lecture		codeconnections:HostArn	
StartOAuthHandshake [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	Lecture		codeconnections:ProviderType	
TagResource	Accorde l'autorisation d'ajouter ou de modifier les balises de la ressource spécifiée	Identification	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises d'une AWS ressource	Identification	Connection		
			Host		
			RepositoryLink		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateConnectionInstallation	Accorde l'autorisation de mettre à jour une ressource Connection avec une installation de l'application CodeStar Connections	Écrire	Connection*		codeconnections:GetIndividualAccessToken codeconnections:GetInstallationUrl codeconnections:ListInstallationTargets codeconnections:StartOAuthHandshake
				codeconnections:InstallationId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateHost	Accorde l'autorisation de mettre à jour une ressource hôte	Écrire	Host*		
				codeconnections:VpcId	
UpdateRepositoryLink	Octroie l'autorisation de mettre à jour un lien de référentiel.	Écrire	RepositoryLink*		
UpdateSyncBlocker	Octroie l'autorisation de mettre à jour un bloqueur de synchronisation de ressource (pile cfn ou autres ressources).	Écrire			
UpdateSyncConfiguration	Octroie l'autorisation de mettre à jour une configuration de synchronisation.	Écrire		codeconnections:Branch	
UseConnection [autorisation uniquement]	Accorde l'autorisation d'utiliser une ressource de connexion pour appeler les actions du fournisseur	Lecture	Connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				codeconnections:BranchName codeconnections:FullRepositoryId codeconnections:OwnerId codeconnections:ProviderAction codeconnections:ProviderPermissionsRequired codeconnections:RepositoryName	

Types de ressources définis par AWS CodeConnections

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Connection	`arn:${Partition}:codeconnections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codeconnections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codeconnections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS CodeConnections

AWS CodeConnections définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
codeconnections:Branch	Filtre l'accès en fonction du nom de la branche transmis dans la demande.	String
codeconnections:BranchName	Filtre l'accès en fonction du nom de la branche transmis dans la demande. S'applique uniquement aux UseConnection demandes d'accès à une branche de référentiel spécifique	String
codeconnections:FullRepositoryId	Filtre l'accès en fonction du référentiel transmis dans la demande. S'applique uniquement aux UseConnection demandes d'accès à un référentiel spécifique	String
codeconnections:HostArn	Filtre l'accès en fonction de la ressource hôte associée à la connexion utilisée dans la demande	ARN
codeconnections:InstallationId	Filtre l'accès en fonction de l'identifiant tiers (tel que l'identifiant d'installation de l'application Bitbucket pour CodeConnections) utilisé pour mettre à jour une connexion. Permet de restreindre les installations d'applications tierces qui peuvent être utilisées pour établir une connexion	Chaîne
codeconnections:OwnerId	Filtre l'accès en fonction du propriétaire du référentiel tiers. S'applique uniquement aux UseConnection demandes d'accès aux référentiels appartenant à un utilisateur spécifique	String
codeconnections:PassedToService	Filtre l'accès par le service auquel le principal est autorisé à transmettre une connexion ou RepositoryLink	String

Clés de condition	Description	Type
codeconnections:ProviderAction	Filtre l'accès en fonction de l'action du fournisseur dans une UseConnection demande telle que ListRepositories. Voir la documentation pour toutes les valeurs valides	String
codeconnections:ProviderPermissionsRequired	Filtre l'accès en fonction des autorisations d'écriture d'une action du fournisseur dans une UseConnection demande. Les types valides incluent read_only et read_write	Chaîne
codeconnections:ProviderType	Filtre l'accès en fonction du type de fournisseur tiers transmis dans la demande	Chaîne
codeconnections:ProviderTypeFilter	Filtre l'accès en fonction du type de fournisseur tiers utilisé pour filtrer les résultats	Chaîne
codeconnections:RepositoryName	Filtre l'accès en fonction du nom du référentiel transmis dans la demande. S'applique uniquement aux UseConnection demandes d'accès aux référentiels appartenant à un utilisateur spécifique	String
codeconnections:VpcId	Filtre l'accès en fonction des VpcId informations transmises dans la demande	String

Actions, ressources et clés de condition pour AWS CodeDeploy

AWS CodeDeploy (préfixe de service :`codedeploy`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CodeDeploy
- Types de ressources définis par AWS CodeDeploy
- Clés de condition pour AWS CodeDeploy

Actions définies par AWS CodeDeploy

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTagsToOnPremisesInstances	Accorde l'autorisation d'ajouter des étiquettes à une ou plusieurs instances sur site.	Identification	instance*		
BatchGetApplicationRevisions	Accorde l'autorisation d'obtenir plus d'informations sur une ou plusieurs révisions d'application.	Lecture	application*		
BatchGetApplications	Accorde l'autorisation d'obtenir des informations sur plusieurs applications associées à l'utilisateur IAM.	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetDeploymentGroups	Accorde l'autorisation d'obtenir des informations sur un ou plusieurs groupes de déploiement.	Lecture	deploymentgroup*		
BatchGetDeploymentInstances	Accorde l'autorisation d'obtenir des informations sur une ou plusieurs instances faisant partie d'un groupe de déploiement.	Lecture	deploymentgroup*		
BatchGetDeploymentTargets	Accorde l'autorisation de renvoyer une matrice d'une ou plusieurs cibles associée à un déploiement. Cette méthode fonctionne avec tous les types de calcul et doit être utilisée à la place de la méthode obsolète BatchGetDeploymentInstances. Le nombre maximal de cibles pouvant être renvoyées est de 25.	Lecture			
BatchGetDeployments	Accorde l'autorisation d'obtenir des informations sur plusieurs déploiements associés à l'utilisateur IAM.	Lecture	deploymentgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetOnPremisesInstances	Accorde l'autorisation d'obtenir des informations sur une ou plusieurs instances sur site.	Lecture	instance*		
ContinueDeployment	Accorde l'autorisation de démarrer le processus de redirection du trafic des instances de l'environnement d'origine vers les instances de l'environnement de remplacement sans attendre que le délai d'attente spécifié soit écoulé.	Écrire			
CreateApplication	Accorde l'autorisation de créer une application associée à l'utilisateur IAM.	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment [autorisation uniquement]	Accorde l'autorisation de créer un CloudFormation déploiement afin de coopérer à l'orchestration d'une mise à jour de la pile CloudFormation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeployment	Accorde l'autorisation de créer un déploiement pour une application associée à l'utilisateur IAM.	Écrire	deploymentgroup*		
CreateDeploymentConfig	Accorde l'autorisation de créer une configuration de déploiement personnalisée associée à l'utilisateur IAM.	Écrire	deploymentconfig*		
CreateDeploymentGroup	Accorde l'autorisation de créer un groupe de déploiement pour une application associée à l'utilisateur IAM.	Écrire	deploymentgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Accorde l'autorisation de supprimer une application associée à l'utilisateur IAM.	Écrire	application*		
DeleteDeploymentConfig	Accorde l'autorisation de supprimer une configuration de déploiement personnalisée associée à l'utilisateur IAM.	Écrire	deploymentconfig*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDeploymentGroup	Accorde l'autorisation de supprimer un groupe de déploiement pour une application associée à l'utilisateur IAM.	Écrire	deploymentgroup*		
DeleteGitHubAccountToken	Accorde l'autorisation de supprimer une connexion à un GitHub compte	Écrire			
DeleteResourcesByExternalId	Accorde l'autorisation de supprimer les ressources associées à l'ID externe donné.	Écrire			
DeregisterOnPremisesInstance	Accorde l'autorisation d'annuler l'enregistrement d'une instance sur site.	Écrire	instance*		
GetApplication	Accorde l'autorisation d'obtenir des informations sur une application individuelle associée à l'utilisateur IAM.	List	application*		
GetApplicationRevision	Accorde l'autorisation d'obtenir des informations sur la révision individuelle d'une application associée à l'utilisateur IAM.	List	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDeployment	Accorde l'autorisation d'obtenir des informations sur un déploiement individuel à un groupe de déploiement pour une application associée à l'utilisateur IAM.	List	deploymentgroup*		
GetDeploymentConfig	Accorde l'autorisation d'obtenir des informations sur une configuration de déploiement individuelle associée à l'utilisateur IAM.	List	deploymentconfig*		
GetDeploymentGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de déploiement individuel pour une application associée à l'utilisateur IAM.	List	deploymentgroup*		
GetDeploymentInstance	Accorde l'autorisation d'obtenir des informations sur une instance individuelle dans un déploiement associé à l'utilisateur IAM.	List	deploymentgroup*		
GetDeploymentTarget	Accorde l'autorisation de renvoyer des informations sur sur une cible de déploiement.	Lecture			
GetOnPremisesInstance	Accorde l'autorisation d'obtenir des informations sur une instance sur site individuelle.	List	instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplicationRevisions	Accorde l'autorisation d'obtenir des informations sur toutes les révisions de l'application pour une application associée à l'utilisateur IAM.	List	application*		
ListApplications	Accorde l'autorisation d'obtenir des informations sur toutes les applications associées à l'utilisateur IAM.	List			
ListDeploymentConfigs	Accorde l'autorisation d'obtenir des informations sur toutes les configurations de déploiement spécifiques associées à l'utilisateur IAM.	List			
ListDeploymentGroups	Accorde l'autorisation d'obtenir des informations sur tous les groupes de déploiement pour une application associée à l'utilisateur IAM.	List	application*		
ListDeploymentInstances	Accorde l'autorisation d'obtenir des informations sur toutes les instances dans un déploiement associé à l'utilisateur IAM.	List	deploymentgroup*		
ListDeploymentTargets	Accorde l'autorisation de renvoyer un tableau de cibles IDs associées à un déploiement	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDeployments	Accorde l'autorisation d'obtenir des informations sur tous les déploiements à un groupe de déploiement associé à l'utilisateur IAM ou d'obtenir tous les déploiements associés à l'utilisateur IAM.	List	deploymentgroup*		
ListGitHubAccountTokenNames	Accorde l'autorisation de répertorier les noms des connexions enregistrées aux GitHub comptes	List			
ListOnPremisesInstances	Accorde l'autorisation d'obtenir une liste d'un ou plusieurs noms d'instances sur site.	List			
ListTagsForResource	Accorde l'autorisation de renvoyer une liste d'étiquettes pour la ressource identifiée par un ARN spécifié. Les tags sont utilisés pour organiser et classer vos ressources CodeDeploy	List	application		
			deploymentgroup		
PutLifecycleEventHookExecutionStatus	Accorde l'autorisation de notifier l'état de l'exécution d'un hook d'événement de cycle de vie pour le déploiement associé à l'utilisateur IAM.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterApplicationRevision	Accorde l'autorisation d'enregistrer des informations sur la révision d'une application pour une application associée à l'utilisateur IAM.	Écrire	application*		
RegisterOnPremisesInstance	Accorde l'autorisation d'enregistrer une instance sur site.	Écrire	instance*		
RemoveTagsFromOnPremisesInstances	Accorde l'autorisation de supprimer les étiquettes d'une ou plusieurs instances sur site.	Identification	instance*		
SkipWaitTimeForInstanceTermination	Accorde l'autorisation d'ignorer tout temps d'attente spécifié et commence à terminer les instances immédiatement après la fin du routage du trafic. Cette action s'applique uniquement aux déploiements bleu/vert.	Écrire			
StopDeployment	Accorde l'autorisation d'arrêter un déploiement	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'associer la liste des balises du paramètre Tags d'entrée à la ressource identifiée par le paramètre ResourceArn d'entrée	Identification	application		
			deploymentgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de dissocier une ressource d'une liste d'étiquettes. La ressource est identifiée par le paramètre ResourceArn d'entrée. Les balises sont identifiées par la liste des clés dans le TagKeys paramètre d'entrée	Identification	application		
			deploymentgroup		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écrire	application*		
UpdateDeploymentGroup	Accorde l'autorisation de modifier les informations sur un groupe de déploiement individuel pour une application associée à l'utilisateur IAM.	Écrire	deploymentgroup*		

Types de ressources définis par AWS CodeDeploy

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:codedeploy:${Region}:${Account}:application:${ApplicationName}`	aws:ResourceTag/${TagKey}
deploymentconfig	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentconfig:${DeploymentConfigurationName}`	
deploymentgroup	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentgroup:${ApplicationName}/${DeploymentGroupName}`	aws:ResourceTag/${TagKey}
instance	`arn:${Partition}:codedeploy:${Region}:${Account}:instance:${InstanceName}`	

Clés de condition pour AWS CodeDeploy

AWS CodeDeploy définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour un service de commandes hôte AWS CodeDeploy sécurisé

AWS CodeDeploy le service de commandes hôte sécurisé (préfixe de service :`codedeploy-commands-secure`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service de commandes AWS CodeDeploy sécurisé de l'hôte
- Types de ressources définis par le service de commandes hôte AWS CodeDeploy sécurisé
- Clés de condition pour le service de commandes hôte AWS CodeDeploy sécurisé

Actions définies par le service de commandes AWS CodeDeploy sécurisé de l'hôte

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDeploymentSpecification	Accorde l'autorisation d'obtenir la spécification de déploiement	Lecture			
PollHostCommand	Accorde l'autorisation de demander des commandes de l'agent hôte	Lecture			
PutHostCommandAcknowledgement	Accorde l'autorisation de marquer les commandes de l'agent hôte comme reconnues	Écrire			
PutHostCommandComplete	Accorde l'autorisation de marquer les commandes de l'agent hôte comme terminées	Écrire			

Types de ressources définis par le service de commandes hôte AWS CodeDeploy sécurisé

AWS CodeDeploy le service de commandes hôte sécurisé ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au service de commandes AWS CodeDeploy sécurisé de l'hôte, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour le service de commandes hôte AWS CodeDeploy sécurisé

CodeDeploy Commands Secure ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon CodeGuru

Amazon CodeGuru (préfixe de service :`codeguru`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CodeGuru
- Types de ressources définis par Amazon CodeGuru
- Clés de condition pour Amazon CodeGuru

Actions définies par Amazon CodeGuru

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCodeGuruFreeTrialSummary [autorisation uniquement]	Accorde l'autorisation d'obtenir un résumé de l'essai gratuit pour le CodeGuru service, y compris la date d'expiration	Lecture			

Types de ressources définis par Amazon CodeGuru

Amazon CodeGuru ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon CodeGuru, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Amazon CodeGuru

CodeGuru ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon CodeGuru Profiler

Amazon CodeGuru Profiler (préfixe de service :`codeguru-profiler`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CodeGuru Profiler
- Types de ressources définis par Amazon CodeGuru Profiler
- Clés de condition pour Amazon CodeGuru Profiler

Actions définies par Amazon CodeGuru Profiler

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddNotificationChannels	Permet d'ajouter jusqu'à 2 sujets parmi les sujets AWS SNS existants pour publier des notifications ARNs	Écrire	ProfilingGroup*		
BatchGetFrameMetricData	OAccorde l'autorisation d'obtenir les données de métrique de trame pour un groupe de profilage	List	ProfilingGroup*		
ConfigureAgent	Accorde l'autorisation de s'inscrire auprès du service d'orchestration et de récupérer les informations de configuration de profilage, utilisées par les agents	Écrire	ProfilingGroup*		
CreateProfilingGroup	Accorde l'autorisation de créer un groupe de profilage	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteProfilingGroup	Accorde l'autorisation de supprimer un groupe de profilage	Écriture	ProfilingGroup*		
DescribeProfilingGroup	Accorde l'autorisation de décrire un groupe de profilage	Lecture	ProfilingGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFindingsReportAccountSummary	Accorde l'autorisation d'obtenir un résumé des recommandations récentes pour chaque groupe de profilage dans le compte	Lecture			
GetNotificationConfiguration	Accorde l'autorisation d'obtention de la configuration de la notification	Lecture	Profiling Group*		
GetPolicy	Accorde l'autorisation d'obtenir la politique de ressources associée au groupe de profilage spécifié	Lecture	Profiling Group*		
GetProfile	Accorde l'autorisation d'obtenir des profils agrégés pour un groupe de profilage spécifique	Lecture	Profiling Group*		
GetRecommendations	Accorde l'autorisation d'obtenir des recommandations	Lecture	Profiling Group*		
ListFindingsReports	Accorde l'autorisation de répertorier les rapports de recommandations disponibles pour un groupe de profilage spécifique	Liste	Profiling Group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProfileTimes	Accorde l'autorisation de répertorier les heures de début des profils agrégés disponibles pour un groupe de profilage spécifique	Liste	Profiling Group*		
ListProfilingGroups	Accorde l'autorisation de répertorier les groupes de profilage dans le compte	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'un groupe de profilage	List	Profiling Group*		
PostAgentProfile	Accorde l'autorisation de soumettre un profil collecté par un agent appartenant à un groupe de profilage spécifique à des fins d'agrégation	Écrire	Profiling Group*		
PutPermission	Accorde l'autorisation de mettre à jour la liste des mandataires autorisés pour un groupe d'actions dans la politique de ressources associée au groupe de profilage spécifié	Gestion des autorisations	Profiling Group*		
RemoveNotificationChannel	Accorde l'autorisation de supprimer un SNStopic ARN déjà configuré dans la configuration des notifications	Écrire	Profiling Group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemovePermission	Accorde l'autorisation de supprimer l'autorisation du groupe d'actions spécifié de la politique de ressources associée au groupe de profilage spécifié	Gestion des autorisations	ProfilingGroup*		
SubmitFeedback	Accorde l'autorisation de soumettre des commentaires d'utilisateur pour une anomalie utile ou inutile	Écriture	ProfilingGroup*		
TagResource	Accorde l'autorisation d'ajouter ou de remplacer des balises dans un groupe de profilage	Balisage	ProfilingGroup*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises d'un groupe de profilage	Balisage	ProfilingGroup*		
				aws:TagKeys	
UpdateProfilingGroup	Accorde l'autorisation de mettre à jour un groupe de profilage spécifique	Écrire	ProfilingGroup*		

Types de ressources définis par Amazon CodeGuru Profiler

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Profiling Group	`arn:${Partition}:codeguru-profiler:${Region}:${Account}:profilingGroup/${ProfilingGroupName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CodeGuru Profiler

Amazon CodeGuru Profiler définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer (préfixe de service :`codeguru-reviewer`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CodeGuru Reviewer
- Types de ressources définis par Amazon CodeGuru Reviewer
- Clés de condition pour Amazon CodeGuru Reviewer

Actions définies par Amazon CodeGuru Reviewer

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate Repository	Accorde l'autorisation d'associer un référentiel à Amazon CodeGuru Reviewer	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	codecommit:GetRepository

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					codecommit:ListRepositories codecommit:TagResource codestar-connections:PassConnection events:PutRule events:PutTargets iam:CreateServiceLinkedRole s3:CreateBucket s3:ListBucket s3:PutBucketPolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					s3:PutLifecycleConfiguration
CreateCodeReview	Accorde l'autorisation de créer une révision de code.	Écriture	association*		s3:GetObject
				aws:ResourceTag/${TagKey}	
CreateConnectionToken [autorisation uniquement]	Accorde l'autorisation d'effectuer une connexion OAuth basée sur le web pour les fournisseurs tiers.	Lecture			
DescribeCodeReview	Accorde l'autorisation de décrire une révision de code.	Lecture	association*		
				aws:ResourceTag/${TagKey}	
DescribeRecommendationFeedback	Accorde l'autorisation de décrire un commentaire de recommandation lors d'une révision de code.	Lecture	association*		
				aws:ResourceTag/${TagKey}	
DescribeRepositoryAssociation	Accorde l'autorisation de décrire une association de référentiel.	Lecture	association*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DisassociateRepository	Accorde l'autorisation de dissocier un référentiel d'Amazon CodeGuru Reviewer	Écrire	association*		codecommit:UntagResource events:DeleteRule events:RemoveTargets
				aws:ResourceTag/${TagKey}	
GetMetricsData [autorisation uniquement]	Accorde l'autorisation d'afficher les métriques de demande d'extraction dans la console.	Lecture			
ListCodeReviews	Accorde l'autorisation de répertorier le récapitulatif des révisions de code.	Liste			
ListRecommendationFeedback	Accorde l'autorisation de répertorier le récapitulatif des commentaires de recommandation lors d'une révision de code.	Liste	association*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ListRecommendations	Accorde l'autorisation de répertorier le récapitulatif des recommandations lors d'une révision de code	Liste	association*		
				aws:ResourceTag/${TagKey}	
ListRepositoryAssociations	Accorde l'autorisation de répertorier le récapitulatif des associations de référentiel.	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier la ressource attachée à un ARN de référentiel associé.	Liste	association*		
				aws:ResourceTag/${TagKey}	
ListThirdPartyRepositories [autorisation uniquement]	Accorde l'autorisation de répertorier les référentiels de fournisseurs tiers dans la console.	Lecture			
PutRecommendationFeedback	Accorde l'autorisation de laisser des commentaires pour une recommandation lors d'une révision de code.	Écriture	association*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation d'attacher des balises de ressource à un ARN de référentiel associé.	Balisage	association*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagResource	Accorde l'autorisation de dissocier les balises de ressource d'un ARN de référentiel associé.	Identification	association*		
				aws:TagKeys	

Types de ressources définis par Amazon CodeGuru Reviewer

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
association	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}`	aws:ResourceTag/${TagKey}
codereview	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}:codereview:${CodeReviewId}`	

Clés de condition pour Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction de la présence de clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon CodeGuru Security

Amazon CodeGuru Security (préfixe de service :`codeguru-security`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CodeGuru Security
- Types de ressources définis par Amazon CodeGuru Security
- Clés de condition pour Amazon CodeGuru Security

Actions définies par Amazon CodeGuru Security

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetFindings	Autorise la récupération par lots de résultats spécifiques générés par CodeGuru Security	Lecture	ScanName*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateScan	Accorde l'autorisation de créer un scan CodeGuru de sécurité	Écrire	ScanName		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUploadUrl	Octroie l'autorisation de générer une URL présignée pour le téléchargement d'archives de code	Écrire	ScanName		
DeleteScansByCategory [autorisation uniquement]	Accorde l'autorisation de supprimer tous les scans et les résultats associés dans la CodeGuru section Sécurité par catégorie donnée	Écrire			
GetAccountConfiguration	Accorde l'autorisation de récupérer les configurations au niveau du compte.	Lecture			
GetFindings	Accorde l'autorisation de récupérer les résultats d'une analyse générée par CodeGuru Security	List	ScanName		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMetricsSummary	Accorde l'autorisation de récupérer le résumé des métriques au niveau du AWS compte généré par Security CodeGuru	Lecture			
GetScan	Accorde l'autorisation de récupérer les métadonnées du scan CodeGuru de sécurité	Lecture	ScanName		
				aws:ResourceTag/${TagKey}	
ListFindings [autorisation uniquement]	Accorde l'autorisation de récupérer les résultats générés par CodeGuru Security	List			
ListFindingsMetrics	Accorde l'autorisation de récupérer une liste de résultats des métriques au niveau du compte à une plage de dates spécifique	List			
ListScans	Accorde l'autorisation de récupérer la liste des métadonnées du scan de CodeGuru sécurité	List			
ListTagsForResource	Accorde l'autorisation de récupérer une liste de balises pour un nom d'analyse ARN	Lecture	ScanName		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation d'ajouter des balises à un nom d'analyse ARN	Identification	ScanName*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises d'un nom d'analyse ARN	Identification	ScanName*		
				aws:TagKeys	
UpdateAccountConfiguration	Octroie l'autorisation de mettre à jour les configurations au niveau du compte	Écrire			

Types de ressources définis par Amazon CodeGuru Security

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
ScanName	`arn:${Partition}:codeguru-security:${Region}:${Account}:scans/${ScanName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CodeGuru Security

Amazon CodeGuru Security définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS CodePipeline

AWS CodePipeline (préfixe de service :`codepipeline`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CodePipeline
- Types de ressources définis par AWS CodePipeline
- Clés de condition pour AWS CodePipeline

Actions définies par AWS CodePipeline

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcknowledgeJob	Accorde l'autorisation d'afficher les informations relatives à une tâche spécifiée et de déterminer si cette tâche a été reçue par l'exécutant de tâches.	Écriture			
AcknowledgeThirdPartyJob	Accorde l'autorisation de confirmer qu'un exécutant de tâches a reçu la tâche	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	spécifiée (actions partenaires uniquement)				
CreateCustomActionType	Accorde l'autorisation de créer une action personnalisée que vous pouvez utiliser dans les pipelines associés à votre Compte AWS	Écrire	actiontype*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Accorde l'autorisation de créer un pipeline nommé de manière unique	Écrire	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomActionType	Accorde l'autorisation de supprimer une action personnalisée	Écriture	actiontype*		
DeletePipeline	Accorde l'autorisation de supprimer un pipeline spécifié	Écriture	pipeline*		
DeleteWebhook	Accorde l'autorisation de supprimer un webhook spécifié	Écriture	webhook*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterWebhookWithThirdParty	Accorde l'autorisation de supprimer l'enregistrement d'un webhook avec le tiers spécifié dans sa configuration	Écriture	webhook*		
DisableStageTransition	Accorde l'autorisation d'empêcher les révisions de passer à l'étape suivante d'un pipeline	Écriture	stage*		
EnableStageTransition	Accorde l'autorisation de permettre aux révisions de passer à l'étape suivante d'un pipeline	Écrire	stage*		
GetActionType	Accorde l'autorisation d'afficher les informations sur un type d'action	Lecture			
GetJobDetails	Accorde l'autorisation d'afficher des informations sur une tâche (actions personnalisées uniquement)	Lecture			
GetPipeline	Accorde l'autorisation de récupérer des informations sur une structure de pipeline	Lecture	pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPipelineExecution	Accorde l'autorisation d'afficher des informations sur une exécution d'un pipeline, ainsi que des informations sur les artefacts, l'ID d'exécution du pipeline, et le nom, la version et l'état du pipeline	Lecture	pipeline*		
GetPipelineState	Accorde l'autorisation d'afficher des informations sur l'état actuel des étapes et des actions d'un pipeline	Lecture	pipeline*		
GetThirdPartyJobDetails	Accorde l'autorisation d'afficher les détails d'une tâche pour une action tierce (actions partenaires uniquement)	Lecture			
ListActionExecutions	Accorde l'autorisation de répertorier les exécutions d'actions qui se sont produites dans un pipeline	Lecture	pipeline*		
ListActionTypes	Accorde l'autorisation de répertorier un récapitulatif de tous les types d'actions disponibles pour les pipelines de votre compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDeployActionExecutionTargets	Accorde l'autorisation de répertorier les détails du déploiement pour les exécutions d'actions de déploiement survenues dans un pipeline	Lecture	pipeline*		
ListPipelineExecutions	Accorde l'autorisation de répertorier un récapitulatif des exécutions les plus récentes d'un pipeline	List	pipeline*		
ListPipelines	Permet de répertorier un résumé de tous les pipelines associés à votre Compte AWS	List			
ListRuleExecutions	Accorde l'autorisation de répertorier les exécutions de règles qui ont eu lieu dans un pipeline	Lecture	pipeline*		
ListRuleTypes	Permet de répertorier un résumé de tous les types de règles disponibles pour les pipelines dans votre compte	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une CodePipeline ressource	Lecture	actiontype		
			pipeline		
			webhook		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWebhooks	Accorde l'autorisation de répertorier tous les webhooks associés à votre Compte AWS	List	webhook*		
OverrideStageCondition	Autorise la reprise de l'exécution du pipeline en remplaçant une condition dans une étape	Écrire	stage*		
PollForJobs	Accorde l'autorisation de consulter les informations relatives à toute offre d'emploi CodePipeline pour y donner suite	Écrire	actiontype*		
PollForThirdPartyJobs	Accorde l'autorisation de déterminer s'il existe des tâches tierces sur lesquelles un exécutant de tâches peut agir (actions partenaires uniquement)	Écriture			
PutActionRevision	Accorde l'autorisation de modifier des actions dans un pipeline	Écrire	action*		
PutApprovalResult	Accorde l'autorisation de fournir une réponse (approuvée ou rejetée) à une demande d'approbation manuelle dans CodePipeline	Écrire	action*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutJobFailureResult	Accorde l'autorisation de représenter l'échec d'une tâche lorsqu'elle est renvoyée au pipeline par un exécutant de tâches (actions personnalisées uniquement)	Écriture			
PutJobSuccessResult	Accorde l'autorisation de représenter la réussite d'une tâche lorsqu'elle est renvoyée au pipeline par un exécutant de tâches (actions personnalisées uniquement)	Écriture			
PutThirdPartyJobFailureResult	Accorde l'autorisation de représenter l'échec d'une tâche tierce lorsqu'elle est renvoyée au pipeline par un exécutant de tâches (actions partenaires uniquement)	Écriture			
PutThirdPartyJobSuccessResult	Accorde l'autorisation de représenter la réussite d'une tâche tierce lorsqu'elle est renvoyée au pipeline par un exécutant de tâches (actions partenaires uniquement)	Écriture			
PutWebhook	Accorde l'autorisation de créer ou de mettre à jour un webhook	Écrire	pipeline* webhook*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterWebhookWithThirdParty	Accorde l'autorisation d'enregistrer un webhook avec le tiers spécifié dans sa configuration.	Écriture	webhook*		
RetryStageExecution	Accorde l'autorisation de reprendre l'exécution d'un pipeline en réessayant les dernières actions d'une étape qui ont échoué	Écrire	stage*		
RollbackStage	Autorise le retour de l'étape à une exécution réussie précédente	Écrire	stage*		
StartPipelineExecution	Accorde l'autorisation d'exécuter la révision la plus récente via le pipeline	Écriture	pipeline*		
StopPipelineExecution	Accorde l'autorisation d'arrêter l'exécution d'un pipeline en cours	Écrire	pipeline*		
TagResource	Accorde l'autorisation de baliser une CodePipeline ressource	Identification	actiontype		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			pipeline		
			webhook		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer un tag d'une CodePipeline ressource	Identification	actiontype		
			pipeline		
			webhook		
				aws:TagKeys	
UpdateActionType	Accorde l'autorisation de mettre à jour un type d'action	Écrire	actiontype*		
UpdatePipeline	Accorde l'autorisation de mettre à jour un pipeline avec les modifications apportées à la structure du pipeline	Écrire	pipeline*		

Types de ressources définis par AWS CodePipeline

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
action	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}/${ActionName}`	aws:ResourceTag/${TagKey}
actiontype	`arn:${Partition}:codepipeline:${Region}:${Account}:actiontype:${Owner}/${Category}/${Provider}/${Version}`	aws:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}`	aws:ResourceTag/${TagKey}
stage	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}`	aws:ResourceTag/${TagKey}
webhook	`arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS CodePipeline

AWS CodePipeline définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS CodeStar

AWS CodeStar (préfixe de service :`codestar`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CodeStar
- Types de ressources définis par AWS CodeStar
- Clés de condition pour AWS CodeStar

Actions définies par AWS CodeStar

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateTeamMember	Accorde l'autorisation d'ajouter un utilisateur à l'équipe pour un AWS CodeStar projet	Gestion des autorisations	project*		
CreateProject	Accorde l'autorisation de créer un projet avec une structure minimale, des stratégies client et aucune ressource	Gestion des autorisations		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Accorde l'autorisation de créer un profil pour un utilisateur incluant les préférences utilisateur, le nom d'affichage et l'e-mail	Écrire	user*		
DeleteExtendedAccess [autorisation uniquement]	Accorde l'autorisation de suppression étendue APIs	Écrire	project*		
DeleteProject	Accorde l'autorisation de supprimer un projet, y compris les ressources de celui-ci. Ne permet pas de supprimer les utilisateurs associés au projet, mais de supprimer les rôles IAM ayant autorisé l'accès au projet	Gestion des autorisations	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteUserProfile	Accorde l'autorisation de supprimer un profil utilisateur dans AWS CodeStar, y compris toutes les données de préférence personnelles associées à ce profil, telles que le nom d'affichage et l'adresse e-mail. Ne permet pas de supprimer l'historique de cet utilisateur, notamment l'historique des validations qu'il a effectuées	Écrire	user*		
DescribeProject	Accorde l'autorisation de décrire un projet et ses ressources	Lecture	project*		
DescribeUserProfile	Accorde l'autorisation de décrire un utilisateur AWS CodeStar et ses attributs dans tous les projets	Lecture			
DisassociateTeamMember	Accorde l'autorisation de supprimer un utilisateur d'un projet. La suppression d'un utilisateur d'un projet supprime également les politiques IAM de cet utilisateur ayant autorisé l'accès au projet et à ses ressources	Gestion des autorisations	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExtendedAccess [autorisation uniquement]	Accorde l'autorisation de lecture prolongée APIs	Lecture	project*		
ListProjects	Accorde l'autorisation de répertorier tous les projets CodeStar associés à votre Compte AWS	List			
ListResources	Accorde l'autorisation de répertorier toutes les ressources associées à un projet dans CodeStar	List	project*		
ListTagsForProject	Accorde l'autorisation de répertorier les balises associées à un projet dans CodeStar	List	project*		
ListTeamMembers	Accorde l'autorisation de répertorier tous les membres d'équipes associés à un projet	List	project*		
ListUserProfiles	Accorde l'autorisation de répertorier les profils utilisateur dans AWS CodeStar	List			
PutExtendedAccess [autorisation uniquement]	Accorde l'autorisation d'écrire de manière prolongée APIs	Écrire	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagProject	Accorde l'autorisation d'ajouter des balises à un projet dans CodeStar	Identification	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagProject	Accorde l'autorisation de supprimer des balises d'un projet dans CodeStar	Identification	project*		
				aws:TagKeys	
UpdateProject	Accorde l'autorisation de mettre à jour un projet dans CodeStar	Écrire	project*		
UpdateTeamMember	Accorde l'autorisation de mettre à jour les attributs des membres de l'équipe dans un CodeStar projet	Gestion des autorisations	project*		
UpdateUserProfile	Accorde l'autorisation de mettre à jour un profil pour un utilisateur incluant les préférences utilisateur, le nom d'affichage et l'e-mail	Écrire	user*		
VerifyServiceRole	Accorde l'autorisation de vérifier si le rôle de AWS CodeStar service existe dans le compte du client	List			

Types de ressources définis par AWS CodeStar

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
project	`arn:${Partition}:codestar:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:iam::${Account}:user/${AwsUserName}`	iam:ResourceTag/${TagKey}

Clés de condition pour AWS CodeStar

AWS CodeStar définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès aux requêtes en fonction de l'ensemble de valeurs autorisées pour chacune des balises	String
aws:ResourceTag/${TagKey}	Filtre l'accès limité par les actions en fonction de la valeur-étiquette associée à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès aux requêtes de création en fonction de la présence de balises obligatoires dans la requête	ArrayOfString
iam:ResourceTag/${TagKey}	Filtre l'accès limité par les actions en fonction de la valeur-étiquette associée à la ressource	String

Actions, ressources et clés de condition pour les AWS CodeStar connexions

AWS CodeStar Connections (préfixe de service :`codestar-connections`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS CodeStar Connections
- Types de ressources définis par AWS CodeStar Connections
- Clés de condition pour les AWS CodeStar connexions

Actions définies par AWS CodeStar Connections

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConnection	Accorde l'autorisation de créer une ressource de connexion.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType	
CreateHost	Accorde l'autorisation de créer une ressource hôte	Écrire		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType codestar-connections:VpcId	
CreateRepositoryLink	Octroie l'autorisation de créer un lien de référentiel.	Écrire	Connection*		codestar-connections:PassConnection

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					codestar-connections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Accorde l'autorisation de créer une config de synchronisation de modèle	Écrire	RepositoryLink*		codestar-connections:PassRepository iam:PassRole
				codestar-connections:Branch	
DeleteConnection	Accorde l'autorisation de supprimer une ressource de connexion.	Écriture	Connection*		
DeleteHost	Accorde l'autorisation de supprimer une ressource hôte.	Écrire	Host*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRepositoryLink	Octroie l'autorisation de supprimer un lien de référentiel.	Écrire	RepositoryLink*		
DeleteSyncConfiguration	Octroie l'autorisation de supprimer une configuration de synchronisation.	Écrire			
GetConnection	Accorde l'autorisation d'obtenir des détails sur une ressource de connexion	Lecture	Connection*		
GetConnectionToken [autorisation uniquement]	Accorde l'autorisation d'obtenir un jeton de connexion pour appeler les actions du fournisseur	Lecture	Connection*		
GetHost	Accorde l'autorisation d'obtenir des détails sur une ressource hôte.	Lecture	Host*		
GetIndividualAccessToken [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	Lecture		codestar-connections:ProviderType	codestar-connections:StartOAuthHandshake
GetInstallationUrl [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	Lecture		codestar-connections:ProviderType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRepositoryLink	Octroie l'autorisation de décrire un lien de référentiel.	Lecture	RepositoryLink*		
GetRepositorySyncStatus	Accorde l'autorisation d'obtenir le dernier statut de synchronisation d'un référentiel	Lecture	RepositoryLink*		
				codestar-connections:Branch	
GetResourceSyncStatus	Octroie l'autorisation d'obtenir le dernier statut de synchronisation d'une ressource (pile cfn ou autres ressources).	Lecture			
GetSyncBlockerSummary	Octroie l'autorisation de décrire les bloqueurs de synchronisation de service sur une ressource (pile cfn ou autres ressources).	Lecture			
GetSyncConfiguration	Octroie l'autorisation de décrire une configuration de synchronisation.	Lecture			
ListConnections	Accorde l'autorisation de répertorier les ressources de connexion	Liste	Connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				codestar-connections:ProviderTypeFilter	
ListHosts	Accorde l'autorisation de répertorier des ressources hôtes	Liste		codestar-connections:ProviderTypeFilter	
ListInstallationTargets [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	List			codestar-connections:GetIndividualAccessToken codestar-connections:StartOAuthHandshake
ListRepositoryLinks	Octroie l'autorisation de répertorier les liens de référentiels.	List			
ListRepositorySyncDefinitions	Accorde l'autorisation de répertorier les définitions de synchronisation de référentiel	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSyncConfigurations	Octroie l'autorisation de répertorier les configurations de synchronisation d'un lien de référentiel.	List			
ListTagsForResource	Accorde l'autorisation d'obtenir l'ensemble des paires clé-valeur utilisées pour gérer la ressource	List	Connection		
			Host		
			RepositoryLink		
PassConnection [autorisation uniquement]	Accorde l'autorisation de transmettre une ressource de connexion à un AWS service qui accepte un ARN de connexion en entrée, tel que codepipeline : CreatePipeline	Lecture	Connection*		
				codestar-connections:PassedToService	
PassRepository [autorisation uniquement]	Accorde l'autorisation de transmettre une ressource de lien de référentiel à un AWS service qui accepte un RepositoryLinkId comme entrée, tel que codestar-connections : CreateSyncConfiguration	Lecture	RepositoryLink*		
				codestar-connections:PassedToService	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterAppCode [autorisation uniquement]	Accorde l'autorisation d'associer un serveur tiers, tel qu'une instance de serveur GitHub d'entreprise, à un hôte	Lecture		codestar-connections:HostArn	
StartAppRegistrationHandshake [autorisation uniquement]	Accorde l'autorisation d'associer un serveur tiers, tel qu'une instance de serveur GitHub d'entreprise, à un hôte	Lecture		codestar-connections:HostArn	
StartOAuthHandshake [autorisation uniquement]	Accorde l'autorisation d'associer un tiers, tel qu'une installation d'application Bitbucket, à une connexion	Lecture		codestar-connections:ProviderType	
TagResource	Accorde l'autorisation d'ajouter ou de modifier les balises de la ressource spécifiée	Identification	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des balises d'une AWS ressource	Identification	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConnectionInstallation	Accorde l'autorisation de mettre à jour une ressource Connection avec une installation de l'application CodeStar Connections	Écrire	Connection*		codestar-connections:GetIndividualAccessToken codestar-connections:GetInstallationUrl codestar-connections:ListInstallationTargets codestar-connections:StartOAuthHandshake
				codestar-connections:InstallationId	
UpdateHost	Accorde l'autorisation de mettre à jour une ressource hôte	Écrire	Host*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				codestar-connections:VpcId	
UpdateRepositoryLink	Octroie l'autorisation de mettre à jour un lien de référentiel.	Écrire	RepositoryLink*		
UpdateSyncBlocker	Octroie l'autorisation de mettre à jour un bloqueur de synchronisation de ressource (pile cfn ou autres ressources).	Écrire			
UpdateSyncConfiguration	Octroie l'autorisation de mettre à jour une configuration de synchronisation.	Écrire		codestar-connections:Branch	
UseConnection [autorisation uniquement]	Accorde l'autorisation d'utiliser une ressource de connexion pour appeler les actions du fournisseur	Lecture	Connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				codestar-connections:BranchName codestar-connections:FullRepositoryId codestar-connections:OwnerId codestar-connections:ProviderAction codestar-connections:ProviderPermissionsRequired codestar-connections:RepositoryName	

Types de ressources définis par AWS CodeStar Connections

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Connection	`arn:${Partition}:codestar-connections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codestar-connections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codestar-connections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les AWS CodeStar connexions

AWS CodeStar Connections définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
codestar-connections:Branch	Filtre l'accès en fonction du nom de la branche transmis dans la demande.	String
codestar-connections:BranchName	Filtre l'accès en fonction du nom de la branche transmis dans la demande. S'applique uniquement aux UseConnection demandes d'accès à une branche de référentiel spécifique	String
codestar-connections:FullRepositoryId	Filtre l'accès en fonction du référentiel transmis dans la demande. S'applique uniquement aux UseConnection demandes d'accès à un référentiel spécifique	String
codestar-connections:HostArn	Filtre l'accès en fonction de la ressource hôte associée à la connexion utilisée dans la demande	ARN
codestar-connections:InstallationId	Filtre l'accès en fonction de l'identifiant tiers (tel que l'identifiant d'installation de l'application Bitbucket pour CodeStar Connections) utilisé pour mettre à jour une connexion. Permet de restreindre les installations d'applications tierces qui peuvent être utilisées pour établir une connexion	Chaîne

Clés de condition	Description	Type
codestar-connections:OwnerId	Filtre l'accès en fonction du propriétaire du référenti el tiers. S'applique uniquement aux UseConnection demandes d'accès aux référentiels appartenant à un utilisateur spécifique	String
codestar-connections:PassedToService	Filtre l'accès par le service auquel le principal est autorisé à transmettre une connexion ou RepositoryLink	String
codestar-connections:ProviderAction	Filtre l'accès en fonction de l'action du fournisseur dans une UseConnection demande telle que ListRepositories. Voir la documentation pour toutes les valeurs valides	String
codestar-connections:ProviderPermissionsRequired	Filtre l'accès en fonction des autorisations d'écriture d'une action du fournisseur dans une UseConnection demande. Les types valides incluent read_only et read_write	Chaîne
codestar-connections:ProviderType	Filtre l'accès en fonction du type de fournisseur tiers transmis dans la demande	Chaîne
codestar-connections:ProviderTypeFilter	Filtre l'accès en fonction du type de fournisseur tiers utilisé pour filtrer les résultats	Chaîne
codestar-connections:RepositoryName	Filtre l'accès en fonction du nom du référentiel transmis dans la demande. S'applique uniquement aux UseConnection demandes d'accès aux référentiels appartenant à un utilisateur spécifique	String

Clés de condition	Description	Type
codestar-connections:VpcId	Filtre l'accès en fonction des VpcId informations transmises dans la demande	String

Actions, ressources et clés de condition pour les AWS CodeStar notifications

AWS CodeStar Les notifications (préfixe de service :`codestar-notifications`) fournissent les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les AWS CodeStar notifications
- Types de ressources définis par AWS CodeStar les notifications
- Clés de condition pour les AWS CodeStar notifications

Actions définies par les AWS CodeStar notifications

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateNotificationRule	Accorde l'autorisation de créer une règle de notification pour une ressource	Écriture	notificationrule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteNotificationRule	Accorde l'autorisation de supprimer une règle de notification pour une ressource	Écriture	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteTarget	OctroAccorde ie l'autorisation de supprimer une cible pour une règle de notification	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
DescribeNotificationRule	Accorde l'autorisation d'obtenir des informations sur une règle de notification	Lecture	notificationrule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
ListEventTypes	Accorde l'autorisation de répertorier les types d'événement de notification	List			
ListNotificationRules	Accorde l'autorisation de répertorier les règles de notification dans un Compte AWS	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises attachées à un ARN de ressource de règle de notification	List	notificationrule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTargets	Accorde l'autorisation de répertorier les cibles des règles de notification pour un Compte AWS	List		aws:RequestTag/${TagKey} aws:TagKeys	
Subscribe	Accorde l'autorisation de créer une association entre une règle de notification et une rubrique Amazon SNS	Écriture	notificationrule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
TagResource	Accorde l'autorisation d'attacher des balises de ressource à un ARN de ressource de règle de notification	Balisage	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Unsubscribe	Accorde l'autorisation de supprimer une association entre une règle de notification et une rubrique Amazon SNS	Écriture	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
UntagResource	Accorde l'autorisation de dissocier les balises de ressource d'un ARN de ressource de règle de notification	Balisage	notificationrule*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNotificationRule	Accorde l'autorisation de modifier une règle de notification pour une ressource	Écrire	notificationrule*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Types de ressources définis par AWS CodeStar les notifications

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
notificationrule	`arn:${Partition}:codestar-notifications:${Region}:${Account}:notificationrule/${NotificationRuleId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les AWS CodeStar notifications

AWS CodeStar Les notifications définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString
codestar-notifications:NotificationsForResource	Filtre l'accès en fonction de l'ARN de la ressource pour laquelle les notifications sont configurées	ARN

Actions, ressources et clés de condition pour Amazon CodeWhisperer

Amazon CodeWhisperer (préfixe de service :`codewhisperer`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon CodeWhisperer
- Types de ressources définis par Amazon CodeWhisperer
- Clés de condition pour Amazon CodeWhisperer

Actions définies par Amazon CodeWhisperer

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux vendus pour la ressource CodeWhisperer de personnalisation	Gestion des autorisations	customization*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateCustomizationPermission [autorisation uniquement]	Accorde l'autorisation d'invoquer AssociateCustomizationPermission sur CodeWhisperer	Écrire	customization*		
				aws:ResourceTag/${TagKey}	
CreateCustomization [autorisation uniquement]	Accorde l'autorisation d'invoquer CreateCustomization sur CodeWhisperer	Écrire	customization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile [autorisation uniquement]	Accorde l'autorisation d'invoquer CreateProfile sur CodeWhisperer	Écrire	profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCustomization [autorisation uniquement]	Accorde l'autorisation d'invoquer DeleteCustomization sur CodeWhisperer	Écrire	customization*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteProfile [autorisation uniquement]	Accorde l'autorisation d'invoquer DeleteProfile sur CodeWhisperer	Écrire	profile*		
				aws:ResourceTag/${TagKey}	
DisassociateCustomizationPermission [autorisation uniquement]	Accorde l'autorisation d'invoquer DisassociateCustomizationPermission sur CodeWhisperer	Écrire	customization*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations [autorisation uniquement]	Accorde l'autorisation d'invoquer GenerateRecommendations sur CodeWhisperer	Lecture			
GetCustomization [autorisation uniquement]	Accorde l'autorisation d'invoquer GetCustomization sur CodeWhisperer	Lecture	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationPermissions [autorisation uniquement]	Accorde l'autorisation d'invoquer ListCustomizationPermissions sur CodeWhisperer	List	customization*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCustomizationVersions [autorisation uniquement]	Accorde l'autorisation d'invoquer ListCustomizationVersions sur CodeWhisperer	List	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizations [autorisation uniquement]	Accorde l'autorisation d'invoquer ListCustomizations sur CodeWhisperer	List	customization*		
ListProfiles [autorisation uniquement]	Accorde l'autorisation d'invoquer ListProfiles sur CodeWhisperer	List			
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation d'invoquer ListTagsForResource sur CodeWhisperer	List	customization		
			profile		
				aws:ResourceTag/${TagKey}	
TagResource [autorisation uniquement]	Accorde l'autorisation d'invoquer TagResource sur CodeWhisperer	Identification	customization		
			profile		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation d'invoquer UntagResource sur CodeWhisperer	Identification	customization profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCustomization [autorisation uniquement]	Accorde l'autorisation d'invoquer UpdateCustomization sur CodeWhisperer	Écrire	customization*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateProfile [autorisation uniquement]	Accorde l'autorisation d'invoquer UpdateProfile sur CodeWhisperer	Écrire	profile*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon CodeWhisperer

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
profile	`arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	aws:ResourceTag/${TagKey}
customization	`arn:${Partition}:codewhisperer:${Region}:${Account}:customization/${Identifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon CodeWhisperer

Amazon CodeWhisperer définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la CodeWhisperer ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Cognito Identity

Amazon Cognito Identity (préfixe de service : `cognito-identity`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Cognito Identity
- Types de ressources définis par Amazon Cognito Identity
- Clés de condition pour Amazon Cognito Identity

Actions définies par Amazon Cognito Identity

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIdentityPool	Accorde l'autorisation de créer un groupe d'identités	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdentities	Accorde l'autorisation de supprimer des identités d'un groupe d'identités. Vous pouvez spécifier une liste de 1 à 60 identités à supprimer	Écriture		cognito-identity:IdentityPoolArn	
DeleteIdentityPool	Accorde l'autorisation de supprimer un groupe d'utilisateurs. Une fois qu'un groupe est supprimé, les utilisateurs ne peuvent plus s'authentifier auprès de celui-ci.	Écriture	identitypool*		
DescribeIdentity	Accorde l'autorisation de renvoyer les métadonnées relatives à l'identité fournie, y compris la date de création	Lecture		cognito-identity:IdentityPoolArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	de l'identité et les connexions liées associées.				
DescribeIdentityPool	Accorde l'autorisation de récupérer des informations détaillées sur un groupe d'identités, y compris son nom, son ID, sa description, la date de sa création, ainsi que le nombre d'utilisateurs actuels	Lecture	identitypool*		
GetCredentialsForIdentity	Accorde l'autorisation de renvoyer des informations d'identification pour l'ID d'identité fourni	Lecture		cognito-identity-unauth:IdentityPoolArn cognito-identity-unauth:AccountId cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetId	Accorde l'autorisation de générer (ou de récupérer) un ID Cognito. La fourniture de connexions multiples crée un compte lié implicite	Écrire		cognito-identity-unauth:IdentityPoolArn cognito-identity-unauth:AccountId cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	
GetIdentityPoolAnalytics	Accorde l'autorisation d'obtenir des données analytiques sur le nombre total d'identités actuel pour tous les fournisseurs d'identités du pool d'identités (IdPs)	Lecture	identitypool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetIdentityPoolDailyAnalytics	Accorde l'autorisation d'obtenir des données analytiques sur le nombre de nouvelles identités et le nombre total d'identités pour tous les fournisseurs d'identités du pool d'identités (IdPs)	Lecture	identitypool*		
GetIdentityPoolRoles	Accorde l'autorisation d'obtenir les rôles pour un groupe d'identités	Lecture	identitypool*		
GetIdentityProviderDailyAnalytics	Accorde l'autorisation d'obtenir des données analytiques sur le nombre de nouvelles identités et le nombre total d'identités pour un fournisseur d'identités du pool d'identités (IdPs)	Lecture	identitypool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOpenIdToken	Accorde l'autorisation de récupérer un jeton OpenID à l'aide d'un ID Cognito connu	Lecture		cognito-identity-unauth:IdentityPoolArn cognito-identity-unauth:AccountId cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	
GetOpenIdTokenForDeveloperIdentity	Accorde l'autorisation d'enregistrer (ou de récupérer) un Cognito IdentityId et un jeton OpenID Connect pour un utilisateur authentifié par votre processus d'authentification principal	Lecture	identitypool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPrincipalTagAttributeMap	Accorde l'autorisation de récupérer les balises relatives au principal d'un groupe d'identités et d'un fournisseur	Lecture	identitypool*		
ListIdentities	Accorde l'autorisation de répertorier les identités d'un groupe d'identités	Liste	identitypool*		
ListIdentityPools	Accorde l'autorisation de répertorier tous les groupes d'identités Cognito enregistrés pour votre compte	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier les balises qui sont assignées à un groupe d'identités Amazon Cognito	Lecture	identitypool		
LookupDeveloperIdentity	Accorde l'autorisation de récupérer l'identité IdentityId associée à un Developer UserIdentifier ou la liste des DeveloperUserIdentifiers associés IdentityId à une identité existante	Lecture	identitypool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
MergeDeveloperIdentities	Accorde l'autorisation de fusionner deux utilisateurs différents IdentityIds, existant dans le même pool d'identités et identifiés par le même fournisseur de développement	Écrire	identitypool*		
SetIdentityPoolRoles	Accorde l'autorisation de définir les rôles d'un groupe d'identités. Ces rôles sont utilisés lors des appels à l' GetCredentialsForIdentity action	Écrire			
SetPrincipalTagAttributeMap	Accorde l'autorisation de définir les balises relatives au principal d'un groupe d'identités et d'un fournisseur. Ces balises sont utilisées lors des appels à l' GetOpenIdToken action	Écrire			
TagResource	Accorde l'autorisation d'attribuer un ensemble de balises à un groupe d'identités Amazon Cognito	Identification	identitypool*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UnlinkDeveloperIdentity	Accorde l'autorisation DeveloperUserIdentifier de dissocier une identité existante	Écrire	identitypool*		
UnlinkIdentity	Accorde l'autorisation de dissocier une identité fédérée d'un compte existant	Écriture		cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées d'un groupe d'identités Amazon Cognito	Balisage	identitypool*		
				aws:TagKeys	
UpdateIdentityPool	Accorde l'autorisation de mettre à jour un groupe d'identités	Écriture	identitypool*		

Types de ressources définis par Amazon Cognito Identity

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
identitypool	`arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Cognito Identity

Amazon Cognito Identity définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de balise dans la requête.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction d'une clé présente dans la demande	ArrayOfString
cognito-identity-auth:AccountId	Filtre l'accès en fonction de l' Compte AWS ID propriétaire pour les utilisateurs authentifiés par le pool d'identités. S'applique aux opérations d'API non authentifiées (publiques)	String

Clés de condition	Description	Type
cognito-identity-auth:IdentityPoolArn	Filtre l'accès en fonction de l'ID du pool d'identités pour un ID d'utilisateur authentifié donné. S'applique aux opérations d'API non authentifiées (publiques)	ARN
cognito-identity-unauth:AccountId	Filtre l'accès en fonction de l' Compte AWS ID propriétaire d'un pool d'identités pour les utilisateurs invités du pool d'identités. S'applique aux opérations d'API non authentifiées (publiques)	String
cognito-identity-unauth:IdentityPoolArn	Filtre l'accès en fonction de l'ID du pool d'identités pour un ID d'identité d'utilisateur invité donné. S'applique aux opérations d'API non authentifiées (publiques)	ARN
cognito-identity:IdentityPoolArn	Filtre l'accès en fonction de l'ID du pool d'identités pour un ID d'identité donné pour DeleteIdentities et DescribeIdentity	ARN

Actions, ressources et clés de condition pour Amazon Cognito Sync

Amazon Cognito Sync (préfixe de service : `cognito-sync`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Cognito Sync
- Types de ressources définis par Amazon Cognito Sync
- Clés de condition pour Amazon Cognito Sync

Actions définies par Amazon Cognito Sync

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BulkPublish	Accorde l'autorisation d'initier une publication en bloc de tous les jeux de données existants pour un groupe d'identités sur le flux configuré	Écrire	identitypool*		
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données spécifique	Écrire	dataset*		
DescribeDataset	Accorde l'autorisation d'obtenir des métadonnées sur un jeu de données par identité et nom du jeu de données	Lecture	dataset*		
DescribeIdentityPoolUsage	Accorde l'autorisation d'obtenir des détails d'utilisation (par exemple, le stockage de données) concernant un groupe d'identités	Lecture	identitypool*		
DescribeIdentityUsage	Accorde l'autorisation d'obtenir des informations d'utilisation pour une identité, notamment	Lecture	identity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	le nombre de jeux de données et l'utilisation des données				
GetBulkPublishDetails	Accorde l'autorisation d'obtenir le statut de la dernière BulkPublish opération pour un pool d'identités	Lecture	identitypool*		
GetCognitoEvents	Accorde l'autorisation d'obtenir les événements et les fonctions Lambda correspondantes associés à un groupe d'identités	Lecture	identitypool*		
GetIdentityPoolConfiguration	Accorde l'autorisation d'obtenir les paramètres de configuration d'un groupe d'identités	Lecture	identitypool*		
ListDatasets	Accorde l'autorisation de répertorier les jeux de données pour une identité	List	dataset*		
ListIdentityPoolUsage	Accorde l'autorisation d'obtenir une liste des groupes d'identités enregistrés avec Cognito	Lecture	identitypool*		
ListRecords	Accorde l'autorisation d'obtenir des enregistrements paginés, qui ont pu être modifiés après un nombre de synchronisations précis pour un jeu de données et une identité	Lecture	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
QueryRecords [autorisation uniquement]	Accorde l'autorisation d'interroger les enregistrements	Lecture			
RegisterDevice	Accorde l'autorisation d'enregistrer un appareil pour recevoir des notifications de synchronisation push	Écrire	identity*		
SetCognitoEvents	Accorde l'autorisation de définir la fonction AWS Lambda pour un type d'événement donné pour un pool d'identités	Écrire	identitypool*		
SetDatasetConfiguration [autorisation uniquement]	Accorde l'autorisation de configurer des jeux de données	Écrire	dataset*		
SetIdentityPoolConfiguration	Accorde l'autorisation de définir la configuration nécessaire pour la synchronisation push	Écrire	identitypool*		
SubscribeToDataset	Accorde l'autorisation de s'abonner pour recevoir des notifications lorsqu'un jeu de données est modifié par un autre appareil	Écrire	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UnsubscribeFromDataset	Accorde l'autorisation de se désabonner de la réception de notifications lorsqu'un jeu de données est modifié par un autre appareil	Écrire	dataset*		
UpdateRecords	Accorde l'autorisation de poster des mises à jour d'enregistrements et d'ajouter et supprimer des enregistrements pour un jeu de données et un utilisateur	Écrire	dataset*		

Types de ressources définis par Amazon Cognito Sync

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
dataset	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}/dataset/${DatasetName}`	

Types de ressources	ARN	Clés de condition
identity	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}`	
identitypool	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}`	

Clés de condition pour Amazon Cognito Sync

Cognito Sync ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Cognito User Pools

Amazon Cognito User Pools (préfixe de service : `cognito-idp`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Cognito User Pools
- Types de ressources définis par Amazon Cognito User Pools
- Clés de condition pour Amazon Cognito User Pools

Actions définies par Amazon Cognito User Pools

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddCustomAttributes	Accorde l'autorisation d'ajouter des attributs utilisateur au schéma du groupe d'utilisateurs	Écrire	userpool*		
AddUserPoolClientSecret	Accorde l'autorisation d'ajouter un nouveau secret à un client confidentiel	Écrire	userpool*		
AdminAddUserToGroup	Accorde l'autorisation d'ajouter un utilisateur à un groupe	Écrire	userpool*		
AdminConfirmSignUp	Accorde l'autorisation de confirmer l'inscription d'un utilisateur sans code de confirmation	Écrire	userpool*		
AdminCreateUser	Accorde l'autorisation de créer des utilisateurs et d'envoyer les messages de bienvenue par e-mail ou SMS	Écrire	userpool*		
AdminDeleteUser	Accorde l'autorisation de supprimer un utilisateur	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AdminDeleteUserAttributes	Accorde l'autorisation de supprimer les attributs d'un utilisateur	Écrire	userpool*		
AdminDisableProviderForUser	Accorde l'autorisation de dissocier un utilisateur de groupe d'utilisateurs d'un utilisateur de fournisseur d'identité (IdP) tiers	Écrire	userpool*		
AdminDisableUser	Accorde l'autorisation de désactiver un utilisateur	Écrire	userpool*		
AdminEnableUser	Accorde l'autorisation d'activer un utilisateur	Écrire	userpool*		
AdminForgetDevice	Accorde l'autorisation d'annuler l'enregistrement des périphériques d'un utilisateur	Écrire	userpool*		
AdminGetDevice	Accorde l'autorisation d'obtenir des informations sur les périphériques d'un utilisateur	Lecture	userpool*		
AdminGetUser	Accorde l'autorisation de rechercher un utilisateur par nom d'utilisateur	Lecture	userpool*		
AdminInitiateAuth	Accorde l'autorisation d'authentifier un utilisateur	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AdminLinkProviderForUser	Accorde l'autorisation d'associer un utilisateur de groupe d'utilisateurs à un utilisateur de fournisseur d'identité (IdP) tiers	Écrire	userpool*		
AdminListDevices	Accorde l'autorisation de répertorier les périphériques mémorisés d'un utilisateur	List	userpool*		
AdminListGroupsForUser	Accorde l'autorisation de répertorier les groupes auxquels un utilisateur appartient	List	userpool*		
AdminListUserAuthEvents	Accorde l'autorisation de répertorier les événements de connexion d'un utilisateur	Lecture	userpool*		
AdminRemoveUserFromGroup	Accorde l'autorisation de supprimer un utilisateur d'un groupe	Écrire	userpool*		
AdminResetUserPassword	Accorde l'autorisation de réinitialiser le mot de passe d'un utilisateur	Écrire	userpool*		
AdminRespondToAuthChallenge	Accorde l'autorisation de répondre à un défi d'authentification lors de l'authentification d'un utilisateur	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AdminSetUserMFAPreference	Accorde l'autorisation de définir la méthode MFA préférée d'un utilisateur	Écrire	userpool*		
AdminSetUserPassword	Accorde l'autorisation de définir le mot de passe d'un utilisateur	Écrire	userpool*		
AdminSetUserSettings	Accorde l'autorisation de définir les paramètres utilisateur d'un utilisateur	Écrire	userpool*		
AdminUpdateAuthEventFeedback	Accorde l'autorisation de mettre à jour les commentaires de sécurité avancés pour un événement d'authentification d'un utilisateur	Écrire	userpool*		
AdminUpdateDeviceStatus	Accorde l'autorisation de mettre à jour l'état des périphériques mémorisés d'un utilisateur	Écrire	userpool*		
AdminUpdateUserAttributes	Accorde l'autorisation de mettre à jour les attributs standard ou personnalisés d'un utilisateur	Écrire	userpool*		
AdminUserGlobalSignOut	Accorde l'autorisation de déconnecter un utilisateur de toutes les sessions	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateSoftwareToken	Accorde l'autorisation de renvoyer un code de clé secrète partagé généré qui est unique pour l'utilisateur	Écrire			
AssociateWebACL [autorisation uniquement]	Accorde l'autorisation d'associer le groupe d'utilisateurs à une AWS ACL Web WAF	Écrire	userpool* webacl*		
ChangePassword	Accorde l'autorisation de modifier le mot de passe pour un utilisateur spécifié dans un groupe d'utilisateurs	Écrire			
ConfirmDevice	Accorde l'autorisation de confirmer le suivi de l'appareil. Cet appel d'API est l'appel qui démarre le suivi de l'appareil	Écrire			
ConfirmForgotPassword	Autorise l'utilisateur à saisir un code de confirmation pour réinitialiser un mot de passe oublié	Écrire			
ConfirmSignUp	Accorde l'autorisation de confirmer l'inscription d'un utilisateur et gère l'alias existant à partir d'un utilisateur précédent	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGroup	Accorde l'autorisation de créer des groupes de groupes d'utilisateurs	Écrire	userpool*		
CreateIdentityProvider	Accorde l'autorisation d'ajouter des fournisseurs d'identité aux groupes d'utilisateurs	Écrire	userpool*		
CreateManagedLoginBranding	Accorde l'autorisation de créer des paramètres de marque pour la connexion gérée et de l'associer à un client d'application	Écrire	userpool*		
CreateResourceServer	Accorde l'autorisation de créer et de configurer des étendues pour les serveurs de ressources OAuth 2.0	Écrire	userpool*		
CreateTerms	Accorde l'autorisation de créer des termes et de les associer à un client d'application	Écrire	userpool*		
CreateUserImportJob	Accorde l'autorisation de créer des tâches d'importation CSV d'utilisateur	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUserPool	Accorde l'autorisation de créer et de définir une politique de mot de passe pour les groupes d'utilisateurs	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateUserPoolClient	Accorde l'autorisation de créer des clients applications d'un groupe d'utilisateurs	Écrire	userpool*		
CreateUserPoolDomain	Accorde l'autorisation d'ajouter des domaines de groupe d'utilisateurs	Écrire	userpool*		
DeleteGroup	Accorde l'autorisation de supprimer un groupe de groupes d'utilisateurs vide	Écrire	userpool*		
DeleteIdentityProvider	Accorde l'autorisation de supprimer un fournisseur d'identité des groupes d'utilisateurs	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteManagedLoginBranding	Accorde l'autorisation de supprimer le style de marque de connexion géré pour n'importe quel client d'application	Écrire	userpool*		
DeleteResourceServer	Accorde l'autorisation de supprimer n'importe quel serveur de ressources OAuth 2.0 des groupes d'utilisateurs	Écrire	userpool*		
DeleteTerms	Accorde l'autorisation de supprimer des termes pour un client d'application	Écrire	userpool*		
DeleteUser	Autorise un utilisateur à se supprimer	Écrire			
DeleteUserAttributes	Accorde l'autorisation de supprimer les attributs d'un utilisateur	Écrire			
DeleteUserPool	Accorde l'autorisation de supprimer des groupes d'utilisateurs	Écrire	userpool*		
DeleteUserPoolClient	Accorde l'autorisation de supprimer un client application d'un groupe d'utilisateurs	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteUserPoolClientSecret	Accorde l'autorisation de supprimer un secret d'une liste de secrets associée à un client	Écrire	userpool*		
DeleteUserPoolDomain	Accorde l'autorisation de supprimer un domaine de groupe d'utilisateurs	Écrire	userpool*		
DescribeIdentityProvider	Accorde l'autorisation de décrire le fournisseur d'identité d'un groupe d'utilisateurs	Lecture	userpool*		
DescribeManagedLoginBranding	Accorde l'autorisation d'obtenir des informations détaillées sur le style de marque de la connexion gérée	Lecture	userpool*		
DescribeManagedLoginBrandingByClient	Accorde l'autorisation d'obtenir des informations détaillées sur le style de marque de la connexion gérée associée à un client d'application	Lecture	userpool*		
DescribeResourceServer	Accorde l'autorisation de décrire n'importe quel serveur de ressources OAuth 2.0	Lecture	userpool*		
DescribeRiskConfiguration	Accorde l'autorisation de décrire les paramètres de configuration des risques des groupes d'utilisateurs et des clients applications	Lecture	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTerms	Accorde l'autorisation d'obtenir des informations détaillées sur les conditions d'utilisation d'un client d'application	Lecture	userpool*		
DescribeUserImportJob	Accorde l'autorisation de décrire une tâche d'importation d'un utilisateur	Lecture	userpool*		
DescribeUserPool	Accorde l'autorisation de décrire des groupes d'utilisateurs	Lecture	userpool*		
DescribeUserPoolClient	Accorde l'autorisation de décrire un client application d'un groupe d'utilisateurs	Lecture	userpool*		
DescribeUserPoolDomain	Accorde l'autorisation de décrire un domaine de groupe d'utilisateurs	Lecture			
DisassociateWebACL [autorisation uniquement]	Accorde l'autorisation de dissocier le groupe d'utilisateurs d'une ACL AWS Web WAF	Écrire	userpool*		
ForgetDevice	Accorde l'autorisation d'oublier l'appareil spécifié	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ForgotPassword	Accorde l'autorisation d'envoyer un message à l'utilisateur final avec un code de confirmation requis pour modifier le mot de passe de l'utilisateur	Écrire			
GetCSVHeader	Accorde l'autorisation de générer des en-têtes pour un fichier .csv d'importation d'utilisateur	Lecture	userpool*		
GetDevice	Accorde l'autorisation d'obtenir l'appareil	Lecture			
GetGroup	Accorde l'autorisation de décrire un groupe de groupes d'utilisateurs	Lecture	userpool*		
GetIdentityProviderByIdentifier	Accorde l'autorisation de corréler l'identifiant de l'IdP d'un groupe d'utilisateurs avec le nom de l'IdP	Lecture	userpool*		
GetLogDeliveryConfiguration	Accorde l'autorisation d'obtenir la configuration détaillée de la journalisation des activités pour un groupe d'utilisateurs	Lecture	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSigningCertificate	Accorde l'autorisation de rechercher des certificats de signature pour les groupes d'utilisateurs	Lecture	userpool*		
GetTokensFromRefreshToken	Autorise la mise à jour des jetons utilisateur avec des jetons d'actualisation	Écrire			
GetUICustomization	Accorde l'autorisation d'accéder aux informations de personnalisation de l'interface utilisateur pour l'interface utilisateur hébergée d'un client	Lecture	userpool*		
GetUser	Accorde l'autorisation d'obtenir les attributs utilisateur et les métadonnées pour un utilisateur	Lecture			
GetUserAttributeVerificationCode	Accorde l'autorisation d'obtenir le code de vérification des attributs utilisateur pour le nom d'attribut spécifié	Lecture			
GetUserPoolMfaConfig	Accorde l'autorisation de rechercher la configuration MFA des groupes d'utilisateurs	Lecture	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWebACLForResource [autorisation uniquement]	Accorde l'autorisation d'obtenir l'ACL Web AWS WAF associée à un groupe d'utilisateurs Amazon Cognito	Lecture	userpool*		
GlobalSignOut	Accorde l'autorisation de déconnecter les utilisateurs de tous les appareils	Écrire			
InitiateAuth	Accorde l'autorisation de lancer le flux d'authentification	Écrire			
ListDevices	Accorde l'autorisation de répertorier les appareils	List			
ListGroups	Accorde l'autorisation de répertorier tous les groupes dans les groupes d'utilisateurs	List	userpool*		
ListIdentityProviders	Accorde l'autorisation de répertorier tous les fournisseurs d'identité dans les groupes d'utilisateurs	List	userpool*		
ListResourceServers	Accorde l'autorisation de répertorier tous les serveurs de ressources dans les groupes d'utilisateurs	List	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourcesForWebACL [autorisation uniquement]	Accorde l'autorisation de répertorier les groupes d'utilisateurs associés à une AWS ACL Web WAF	List	webacl*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises qui sont assignées à un groupe d'utilisateurs Amazon Cognito	List	userpool		
ListTerms	Accorde l'autorisation de répertorier tous les termes d'un groupe d'utilisateurs	List	userpool*		
ListUserImportJobs	Accorde l'autorisation de répertorier toutes les tâches d'importation d'utilisateur	List	userpool*		
ListUserPoolClientSecrets	Permet de répertorier tous les secrets associés à un client	List	userpool*		
ListUserPoolClients	Accorde l'autorisation de répertorier tous les clients applications dans les groupes d'utilisateurs	List	userpool*		
ListUserPools	Accorde l'autorisation de répertorier tous les groupes d'utilisateurs	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListUsers	Accorde l'autorisation de répertorier tous les utilisateurs du groupe d'utilisateurs	List	userpool*		
ListUsersInGroup	Accorde l'autorisation de répertorier les utilisateurs dans un groupe	List	userpool*		
ResendConfirmationCode	Accorde l'autorisation de renvoyer la confirmation (pour la confirmation d'enregistrement) à un utilisateur spécifique dans le groupe d'utilisateurs	Écrire			
RespondToAuthChallenge	Accorde l'autorisation de répondre à un défi d'authentification	Écrire			
RevokeToken	Accorde l'autorisation de révoquer tous les jetons d'accès générés par le jeton d'actualisation spécifié	Écrire			
SetLogDeliveryConfiguration	Accorde l'autorisation de configurer ou de modifier la configuration détaillée de la journalisation des activités d'un groupe d'utilisateurs	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetRiskConfiguration	Accorde l'autorisation de définir la configuration des risques pour les groupes d'utilisateurs et les clients applications	Écrire	userpool*		
SetUICustomization	Accorde l'autorisation de personnaliser l'interface utilisateur hébergée pour un client application	Écrire	userpool*		
SetUserMFAPreference	Accorde l'autorisation de définir la préférence MFA pour l'utilisateur dans le groupe d'utilisateurs	Écrire			
SetUserPoolMfaConfig	Accorde l'autorisation de définir la configuration MFA du groupe d'utilisateurs	Écrire	userpool*		
SetUserSettings	Accorde l'autorisation de définir les paramètres utilisateur, tels que l'authentification multifactorielle (MFA)	Écrire			
SignUp	Accorde l'autorisation d'enregistrer l'utilisateur dans le groupe d'utilisateurs spécifié et crée un nom d'utilisateur, un mot de passe et des attributs utilisateur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartUserImportJob	Accorde l'autorisation de démarrer une tâche d'importation d'un utilisateur	Écrire	userpool*		
StopUserImportJob	Accorde l'autorisation d'arrêter une tâche d'importation d'un utilisateur	Écrire	userpool*		
TagResource	Accorde l'autorisation de placer une identification sur un groupe d'utilisateurs	Identification	userpool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer l'identification d'un groupe d'utilisateurs	Identification	userpool		
				aws:TagKeys	
UpdateAuthEventFeedback	Accorde l'autorisation de mettre à jour le commentaire pour l'événement d'authentification d'utilisateur	Écrire	userpool*		
UpdateDeviceStatus	Accorde l'autorisation de mettre à jour le statut du périphérique	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGroup	Accorde l'autorisation de mettre à jour la configuration d'un groupe	Écrire	userpool*		
UpdateIdentityProvider	Accorde l'autorisation de mettre à jour la configuration d'un groupe d'utilisateurs IdP	Écrire	userpool*		
UpdateManagedLoginBranding	Accorde l'autorisation de mettre à jour les paramètres de marque d'une connexion gérée	Écrire	userpool*		
UpdateResourceServer	Accorde l'autorisation de mettre à jour la configuration de n'importe quel serveur de ressources OAuth 2.0	Écrire	userpool*		
UpdateTerms	Accorde l'autorisation de mettre à jour les conditions d'un client d'application	Écrire	userpool*		
UpdateUserAttributes	Autorise un utilisateur à mettre à jour un attribut spécifique (un par un)	Écrire			
UpdateUserPool	Accorde l'autorisation de mettre à jour la configuration des groupes d'utilisateurs	Écrire	userpool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateUserPoolClient	Accorde l'autorisation de mettre à jour un client groupe d'utilisateurs	Écrire	userpool*		
UpdateUserPoolDomain	Accorde l'autorisation de remplacer le certificat pour un domaine personnalisé	Écrire	userpool*		
VerifySoftwareToken	Accorde l'autorisation d'enregistrer le code TOTP saisi d'un utilisateur et marque le statut MFA du jeton logiciel de l'utilisateur comme vérifié en cas de succès	Écrire			
VerifyUserAttribute	Accorde l'autorisation de vérifier un attribut utilisateur à l'aide d'un code de vérification à usage unique	Écrire			

Types de ressources définis par Amazon Cognito User Pools

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	aws:ResourceTag/${TagKey}
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	

Clés de condition pour Amazon Cognito User Pools

Amazon Cognito User Pools définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction d'une clé présente dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Comprehend

Amazon Comprehend (préfixe de service : `comprehend`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Comprehend
- Types de ressources définis par Amazon Comprehend
- Clés de condition pour Amazon Comprehend

Actions définies par Amazon Comprehend

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDetectDominantLanguage	Accorde l'autorisation de détecter la ou les langues présentes dans la liste des documents texte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDetectEntities	Accorde l'autorisation de détecter des entités nommées (« Personnes », « Emplacements », « Lieux », etc.) dans la liste des documents texte fournie	Lecture			
BatchDetectKeyPhrases	Accorde l'autorisation de détecter, dans la liste des documents texte, les expressions qui sont les plus révélatrices du contenu	Lecture			
BatchDetectSentiment	Accorde l'autorisation de détecter le sentiment émanant d'un texte dans la liste des documents (positif, négatif, neutre ou mixte).	Lecture			
BatchDetectSyntax	Accorde l'autorisation de détecter des informations syntaxiques (comme la partie vocale, les jetons) dans une liste de documents texte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDetectTargetedSentiment	Accorde l'autorisation de détecter les sentiments associés à des entités spécifiques (telles que des marques ou des produits) dans une liste donnée de documents texte	Lecture			
ClassifyDocument	Accorde l'autorisation de créer une demande de classification de document pour analyser un document unique en temps réel à l'aide d'un modèle personnalisé préalablement créé et entraîné, ainsi que d'un point de terminaison.	Lecture	document-classifier-endpoint*		
ContainsPiiEntities	Accorde l'autorisation de classer en temps réel les informations personnelles identifiables dans des documents donnés	Lecture			
CreateDataset	Octroie l'autorisation de créer un jeu de données dans un volant d'inertie	Écrire	flywheel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDocumentClassifier	Accorde l'autorisation de créer un classificateur de documents que vous pouvez utiliser pour catégoriser des documents	Écriture	document-classifier*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEndpoint	Accorde l'autorisation de créer un point de terminaison spécifique au modèle pour l'inférence synchrone pour un modèle personnalisé préalablement entraîné	Écriture	document-classifier*		
			document-classifier-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			entity-recognizer*		
			entity-recognizer-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			flywheel		
CreateEntityRecognizer	Accorde l'autorisation de créer un module de reconnaissance d'entité à l'aide des fichiers soumis	Écrire	entity-recognizer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFlywheel	Octroie l'autorisation de créer un nouveau volant d'inertie que vous pouvez utiliser pour entraîner des versions de modèles	Écrire	flywheel*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:DataLakeKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDocumentClassifier	Accorde l'autorisation de supprimer un classificateur de documents précédemment créé	Écriture	document-classifier*		
DeleteEndpoint	Accorde l'autorisation de supprimer un point de terminaison spécifique au modèle pour un modèle personnalisé déjà entraîné. Tous les points de terminaison doivent être supprimés pour que le modèle soit supprimé.	Écriture	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DeleteEntityRecognizer	Accorde l'autorisation de supprimer un module de reconnaissance d'entité soumis	Écrire	entity-recognizer*		
DeleteFlywheel	Octroie l'autorisation de supprimer un volant d'inertie	Écrire	flywheel*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique d'une ressource.	Écrire	document-classifier*		
			entity-recognizer*		
DescribeDataset	Octroie l'autorisation d'obtenir les propriétés associées à un jeu de données	Lecture	flywheel-dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDocumentClassificationJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de classification de documents	Lecture	document-classification-job*		
DescribeDocumentClassifier	Accorde l'autorisation d'obtenir les propriétés associées à un classificateur de documents	Lecture	document-classifier*		
DescribeDominantLanguageDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection de langue dominante	Lecture	dominant-language-detection-job*		
DescribeEndpoint	Accorde l'autorisation d'obtenir les propriétés associées à un point de terminaison spécifique. Utilisez cette opération pour obtenir le statut d'un point de terminaison.	Lecture	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DescribeEntitiesDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection d'entités	Lecture	entities-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEntityRecognizer	Accorde l'autorisation de fournir les détails relatifs à un module de reconnaissance d'entités, y compris le statut, les compartiments S3 contenant les données d'entraînement, les métadonnées du module de reconnaissance, les métriques, etc.	Lecture	entity-recognizer*		
DescribeEventsDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection d'événements.	Lecture	events-detection-job*		
DescribeFlywheel	Octroie l'autorisation d'obtenir les propriétés associées à un volant d'inertie	Lecture	flywheel*		
DescribeFlywheelIteration	Octroie l'autorisation d'obtenir les propriétés associées à l'itération d'un volant d'inertie pour un volant d'inertie	Lecture	flywheel*		
				comprehend:FlywheelIterationId	
DescribeKeyPhrasesDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection d'expressions clés	Lecture	key-phrases-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribePiiEntitiesDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection d'entités PII	Lecture	pii-entities-detection-job*		
DescribeResourcePolicy	Accorde l'autorisation de lire la politique attachée sur une ressource	Lecture	document-classifier*		
			entity-recognizer*		
DescribeSentimentDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection de sentiment	Lecture	sentiment-detection-job*		
DescribeTargetedSentimentDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection ciblée des sentiments	Lecture	targeted-sentiment-detection-job*		
DescribeTopicsDetectionJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche de détection de rubrique	Lecture	topics-detection-job*		
DetectDominantLanguage	Accorde l'autorisation de détecter la ou les langues présentes dans le texte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DetectEntities	Accorde l'autorisation de détecter les entités nommées (« Personnes », « Lieux », « Emplacements », etc.) dans le document texte donné	Lecture	entity-recognizer-endpoint		
DetectKeyPhrases	Accorde l'autorisation de détecter les expressions textuelles sont les plus révélatrices du contenu	Lecture			
DetectPiiEntities	Accorde l'autorisation de détecter les entités d'information personnellement identifiables (« Nom », « SSN », « PIN », etc.) dans le document texte donné	Lecture			
DetectSentiment	Accorde l'autorisation de détecter le sentiment d'un texte dans un document (positif, négatif, neutre ou mixte)	Lecture			
DetectSyntax	Accorde l'autorisation de détecter d'informations syntaxiques (comme la partie vocale, les jetons) dans un document texte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DetectTargetedSentiment	Accorde l'autorisation de détecter les sentiments associés à des entités spécifiques (telles que des marques ou des produits) dans un document	Lecture			
DetectToxicContent	Autorise la détection de contenus toxiques dans la liste donnée de segments de texte	Lecture			
ImportModel	Accorde l'autorisation d'importer un modèle Comprehend formé	Écrire	document-classifier*		
			entity-recognizer*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:ModelKmsKey	
ListDatasets	Octroie l'autorisation d'obtenir une liste des jeux de données associés à un volant d'inertie	Lecture	flywheel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDocumentClassificationJobs	Accorde l'autorisation d'obtenir une liste des tâches de classification de documents que vous avez soumises	Lecture			
ListDocumentClassifierSummaries	Accorde l'autorisation d'obtenir une liste de résumés des classificateurs de documents que vous avez créés	Lecture			
ListDocumentClassifiers	Accorde l'autorisation d'obtenir une liste des classificateurs de documents que vous avez créés	Lecture			
ListDominantLanguageDetectionJobs	Accorde l'autorisation d'obtenir une liste des tâches de détection de langue dominante que vous avez soumises	Lecture			
ListEndpoints	Accorde l'autorisation d'obtenir une liste de tous les points de terminaison existants que vous avez créés	Lecture			
ListEntitiesDetectionJobs	Accorde l'autorisation d'obtenir une liste des tâches de détection d'entités que vous avez soumises	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEntityRecognizerSummaries	Accorde l'autorisation d'obtenir une liste de résumés des modules de reconnaissance d'entités que vous avez créés	Lecture			
ListEntityRecognizers	Accorde l'autorisation d'obtenir une liste des propriétés de tous les modules de reconnaissance d'entités créés, y compris ceux en cours d'entraînement.	Lecture			
ListEventsDetectionJobs	Accorde l'autorisation d'obtenir une liste de tâches de détection d'événements que vous avez soumises.	Lecture			
ListFlywheelIterationHistory	Octroie l'autorisation d'obtenir une liste des itérations associées à un volant d'inertie	Lecture	flywheel*		
ListFlywheels	Octroie l'autorisation d'obtenir une liste des volants d'inertie que vous avez créés	Lecture			
ListKeyPhrasesDetectionJobs	Accorde l'autorisation d'obtenir une liste des tâches de détection d'expressions clés que vous avez envoyées	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPiiEntitiesDetectionJobs	Accorde l'autorisation d'obtenir une liste des tâches de détection d'entités PII que vous avez soumises	Lecture			
ListSentimentDetectionJobs	Accorde l'autorisation d'obtenir une liste des tâches de détection de ressenti que vous avez soumises	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			topics-detection-job		
ListTargetedSentimentDetectionJobs	Accorde l'autorisation d'obtenir une liste des tâches de détection ciblée des sentiments que vous avez soumises	Lecture			
ListTopicsDetectionJobs	Accorde l'autorisation d'obtenir une liste des tâches de détection de rubrique que vous avez soumises	Lecture			
PutResourcePolicy	Accorde l'autorisation d'attacher une politique à une ressource	Écrire	document-classifier*		
			entity-recognizer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDocumentClassificationJob	Accorde l'autorisation de démarrer une tâche de classification de document asynchrone	Écriture	document-classification-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			flywheel		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDominantLanguageDetectionJob	Accorde l'autorisation de démarrer une tâche de détection de langue dominante asynchrone pour un ensemble de documents	Écriture	dominant-language-detection-job*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartEntitiesDetectionJob	Accorde l'autorisation de démarrer une tâche de détection d'entités asynchrone pour un ensemble de documents	Écriture	entities-detection-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			entity-recognizer		
			flywheel		
StartEventsDetectionJob	Autorise le démarrage d'une tâche de détection d'événements asynchrone pour un ensemble de documents	Écrire	events-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartFlywheelIteration	Octroie l'autorisation de lancer une itération de volant d'inertie pour un volant d'inertie	Écrire	flywheel*		
StartKeyPhrasesDetectionJob	Accorde l'autorisation de démarrer une tâche de détection d'expressions clés asynchrone pour un ensemble de documents	Écriture	key-phrases-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartPiiEntitiesDetectionJob	Accorde l'autorisation de démarrer une tâche de détection d'entités PII asynchrone pour un ensemble de documents	Écriture	pii-entities-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartSentimentDetectionJob	Accorde l'autorisation de démarrer une tâche de détection de sentiment asynchrone pour un ensemble de documents	Écrire	sentiment-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTargetedSentimentDetectionJob	Accorde l'autorisation de démarrer une tâche asynchrone de détection ciblée des sentiments pour une collection de documents	Écrire	targeted-sentiment-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartTopicsDetectionJob	Accorde l'autorisation de démarrer une tâche asynchrone pour détecter les rubriques les plus courantes dans l'ensemble de documents et les expressions associées à chaque rubrique	Écriture	topics-detection-job*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StopDominantLanguageDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection de langue dominante	Écriture	dominant-language-detection-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopEntitiesDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection d'entités	Écriture	entities-detection-job*		
StopEventsDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection d'événements	Écriture	events-detection-job*		
StopKeyPhrasesDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection d'expressions clés	Écriture	key-phrases-detection-job*		
StopPiiEntitiesDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection d'entités PII	Écriture	pii-entities-detection-job*		
StopSentimentDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection de sentiment	Écrire	sentiment-detection-job*		
StopTargetedSentimentDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection ciblée des sentiments	Écrire	targeted-sentiment-detection-job*		
StopTrainingDocumentClassifier	Accorde l'autorisation d'arrêter une tâche d'entraînement de classificateur de documents déjà créée	Écriture	document-classifier*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopTrainingEntityRecognizer	Accorde l'autorisation d'arrêter une tâche d'entraînement du module de reconnaissance d'entités créée précédemment	Écriture	entity-recognizer*		
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Balisage	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource avec une clé donnée	Balisage	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateEndpoint	Accorde l'autorisation de mettre à jour les informations sur le point de terminaison spécifié	Écrire	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
			flywheel		
UpdateFlywheel	Octroie l'autorisation de mettre à jour la configuration d'un volant d'inertie	Écrire	flywheel*	comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			entity-recognizer		

Types de ressources définis par Amazon Comprehend

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
targeted-sentiment-detection-job	`arn:${Partition}:comprehend:${Region}:${Account}:targeted-sentiment-detection-job/${JobId}`	aws:ResourceTag/${TagKey}
document-classifier	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier/${DocumentClassifierName}`	aws:ResourceTag/${TagKey}
document-classifier-endpoint	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier-endpoint/${DocumentClassifierEndpointName}`	aws:ResourceTag/${TagKey}
entity-recognizer	`arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer/${EntityRecognizerName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
entity-recognizer-endpoint	arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer-endpoint/${EntityRecognizerEndpointName}	aws:ResourceTag/${TagKey}
dominant-language-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:dominant-language-detection-job/${JobId}	aws:ResourceTag/${TagKey}
entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
pii-entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:pii-entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
events-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:events-detection-job/${JobId}	aws:ResourceTag/${TagKey}
key-phrases-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:key-phrases-detection-job/${JobId}	aws:ResourceTag/${TagKey}
sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
topics-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:topics-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classification-job	arn:${Partition}:comprehend:${Region}:${Account}:document-classification-job/${JobId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
flywheel	`arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}`	aws:ResourceTag/${TagKey}
flywheel-dataset	`arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}/dataset/${DatasetName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Comprehend

Amazon Comprehend définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en exigeant des valeurs d'identification présentes dans une demande de création de ressources	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence d'identifications obligatoires dans la demande	ArrayOfString
comprehend:DataLakeKmsKey	Filtre l'accès par la clé DataLake Kms associée à la ressource volant dans la requête	ARN

Clés de condition	Description	Type
comprehend:FlywheelIterationId	Filtre l'accès en fonction de l'ID d'itération spécifique d'un volant d'inertie	String
comprehend:ModelKmsKey	Filtre l'accès en fonction de la clé KMS de modèle associée à la ressource dans la demande	ARN
comprehend:OutputKmsKey	Filtre l'accès en fonction de la clé KMS de sortie associée à la ressource dans la demande	ARN
comprehend:VolumeKmsKey	Filtre l'accès en fonction de la clé KMS de volume associée à la ressource dans la demande	ARN
comprehend:VpcSecurityGroupIds	Filtre l'accès en fonction de la liste de tous les ID de groupe de sécurité VPC associés à la ressource dans la demande	ArrayOfString
comprehend:VpcSubnets	Filtre l'accès en fonction de la liste de tous les sous-rése aux VPC associés à la ressource dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Comprehend Medical

Amazon Comprehend Medical (préfixe de service : `comprehendmedical`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Comprehend Medical

- Types de ressources définis par Amazon Comprehend Medical
- Clés de condition pour Amazon Comprehend Medical

Actions définies par Amazon Comprehend Medical

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEntitiesDetectionV2Job	Accorde l'autorisation de décrire les propriétés d'une tâche de détection d'entités médicales que vous avez soumise	Lecture			
DescribeICD10CMInferenceJob	Accorde l'autorisation de décrire les propriétés d'une tâche de liaison ICD-10-CM que vous avez soumise	Lecture			
DescribePHIDetectionJob	Accorde l'autorisation de décrire les propriétés d'une tâche de détection d'entités PHI que vous avez soumise	Lecture			
DescribeRxNormInferenceJob	Accorde l'autorisation de décrire les propriétés d'une tâche de RxNorm liaison que vous avez soumise	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSNOMEDCTInferenceJob	Accorde l'autorisation de décrire les propriétés d'une tâche de liaison SNOMED-CT que vous avez soumise	Lecture			
DetectEntitiesV2	Accorde l'autorisation de détecter les entités médicales nommées, ainsi que leurs relations et caractéristiques dans le document texte donné	Lecture			
DetectPHI	Accorde l'autorisation de détecter les entités de données de santé protégées (PHI) dans le document texte donné	Lecture			
InferICD10CM	Accorde l'autorisation de détecter les entités d'état de santé dans le document texte donné et de les lier aux codes ICD-10-CM	Lecture			
InferRxNorm	Autorise à détecter les entités médicamenteuses dans le document texte donné et à les relier aux identificateurs conceptuels RxCUI de la base de données de la National Library of Medicine RxNorm	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InferSNOMEDCT	Accorde l'autorisation de détecter les entités de condition médicale, d'anatomie, de test, de traitement et de procédure dans le document texte donné et de les lier aux codes SNOMED-CT	Lecture			
ListEntitiesDetectionV2Jobs	Accorde l'autorisation de répertorier les tâches de détection d'entités médicales que vous avez soumises	Lecture			
ListICD10CMInferenceJobs	Accorde l'autorisation de répertorier les tâches de liaison ICD-10-CM que vous avez soumises	Lecture			
ListPHIDetectionJobs	Accorde l'autorisation de répertorier les tâches de détection d'entités PHI que vous avez soumises	Lecture			
ListRxNormInferenceJobs	Accorde l'autorisation de RxNorm répertorier les tâches de liaison que vous avez soumises	Lecture			
ListSNOMEDCTInferenceJobs	Accorde l'autorisation de répertorier les tâches de liaison SNOMED-CT que vous avez soumises	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartEntitiesDetectionV2Job	Accorde l'autorisation de démarrer une tâche de détection d'entités médicales asynchrone pour un ensemble de documents	Écriture			
StartICD10CMInferenceJob	Accorde l'autorisation de démarrer une tâche de liaison ICD-10-CM asynchrone pour un ensemble de documents	Écriture			
StartPHIDetectionJob	Accorde l'autorisation de démarrer une tâche de détection d'entités PHI asynchrone pour un ensemble de documents	Écrire			
StartRxNormInferenceJob	Accorde l'autorisation de démarrer une tâche de RxNorm liaison asynchrone pour une collection de documents	Écrire			
StartSNOMEDCTInferenceJob	Accorde l'autorisation de démarrer une tâche de liaison SNOMED-CT asynchrone pour un ensemble de documents	Écrire			
StopEntitiesDetectionV2Job	Accorde l'autorisation d'arrêter une tâche de détection d'entités médicales	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopICD10CMInferenceJob	Accorde l'autorisation d'arrêter une tâche de liaison ICD-10-CM	Écriture			
StopPHIDetectionJob	Accorde l'autorisation d'arrêter une tâche de détection d'entités PHI	Écrire			
StopRxNormInferenceJob	Autorise l'arrêt d'une tâche de RxNorm liaison	Écrire			
StopSNOMEDCTInferenceJob	Accorde l'autorisation d'arrêter une tâche de liaison SNOMED-CT	Écrire			

Types de ressources définis par Amazon Comprehend Medical

Amazon Comprehend Medical ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon Comprehend Medical, indiquez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Amazon Comprehend Medical

Amazon Comprehend Medical définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identif ication dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Compute Optimizer

AWS Compute Optimizer (préfixe de service :`compute-optimizer`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Compute Optimizer
- Types de ressources définis par AWS Compute Optimizer
- Clés de condition pour AWS Compute Optimizer

Actions définies par AWS Compute Optimizer

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRecommendationPreferences	Accorde l'autorisation de supprimer les préférences de recommandation	Écrire		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
DescribeRecommendationExportJobs	Accorde l'autorisation d'afficher l'état des tâches d'exportation des recommandations	List			
ExportAutoScalingGroupRecommendations	Autorise l'exportation des recommandations de AutoScaling groupe vers S3 pour les comptes fournis	Écrire			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoSc

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					alingGroupRecommendations
ExportEBSVolumeRecommendations	Accorde l'autorisation d'exporter les recommandations de volume EBS vers S3 pour les comptes fournis	Écriture			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes
ExportEC2InstanceRecommendations	Accorde l'autorisation d'exporter les recommandations d'instance EC2 vers S3 pour les comptes fournis	Écrire			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportECSServiceRecommendations	Accorde l'autorisation d'exporter les recommandations de service ECS vers S3 pour les comptes fournis	Écrire			compute-optimizer:GetECSServiceRecommendations ecs:ListClusters ecs:ListServices
ExportIdleRecommendations	Autorise l'exportation des recommandations inactives vers S3 pour les comptes fournis	Écrire			compute-optimizer:GetIdleRecommendations

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportLambdaFunctionRecommendations	Accorde l'autorisation d'exporter les recommandations de fonction Lambda vers S3 pour les comptes fournis	Écrire			compute-optimizer:GetLambdaFunctionRecommendations lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
ExportLicenseRecommendations	Accorde l'autorisation d'exporter les recommandations de licence vers S3 pour le ou les comptes fournis	Écrire			compute-optimizer:GetLicenseRecommendations ec2:DescribeInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportRDSDatabaseRecommendations	Autorise l'exportation des recommandations RDS vers S3 pour les comptes fournis	Écrire			compute-optimizer:GetRDSDatabaseRecommendations rds:DescribeDBClusters rds:DescribeDBInstances
GetAutoScalingGroupRecommendations	Accorde l'autorisation d'obtenir des recommandations pour les AutoScaling groupes fournis	List			autoscaling:DescribeAutoScalingGroups
GetEBSVolumeRecommendations	Accorde l'autorisation d'obtenir des recommandations pour les volumes EBS fournis	Liste			ec2:DescribeVolumes
GetEC2InstanceRecommendations	Accorde l'autorisation d'obtenir des recommandations pour les instances EC2 fournies	Liste			ec2:DescribeInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEC2RecommendationProjectedMetrics	Accorde l'autorisation d'obtenir les métriques projetées recommandées de l'instance spécifiée	List			ec2:DescribeInstances
GetECSServiceRecommendationProjectedMetrics	Accorde l'autorisation d'obtenir les métriques projetées recommandées du service ECS spécifié	List			
GetECSServiceRecommendations	Accorde l'autorisation d'obtenir des recommandations pour les services ECS fournis	List			ecs:ListClusters ecs:ListServices

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEffectiveRecommendationPreferences	Accorde l'autorisation d'obtenir les préférences de recommandation en vigueur	Lecture		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
GetEnrollmentStatus	Accorde l'autorisation d'obtenir le statut d'inscription du compte spécifié	List			
GetEnrollmentStatusesForOrganization	Accorde l'autorisation d'obtenir les statuts d'inscription des comptes membres de l'organisation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetIdleRecommendations	Accorde l'autorisation d'obtenir des recommandations inactives pour le ou les comptes spécifiés	List			
GetLambdaFunctionRecommendations	Accorde l'autorisation d'obtenir des recommandations pour les fonctions Lambda fournies	List			lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
GetLicenseRecommendations	Accorde l'autorisation d'obtenir les recommandations de licence pour le ou les comptes spécifiés	List			ec2:DescribeInstances
GetRDSDatabaseRecommendationProjectedMetrics	Accorde l'autorisation d'obtenir les métriques projetées recommandées de l'instance spécifiée	List			rds:DescribeDBClusters rds:DescribeDBInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRDSDatabaseRecommendations	Accorde l'autorisation d'obtenir des recommandations RDS pour le ou les comptes spécifiés	List			rds:DescribeDBClusters rds:DescribeDBInstances
GetRecommendationPreferences	Accorde l'autorisation d'obtenir les préférences de recommandation	Lecture		compute-optimizer:ResourceType	
GetRecommendationSummaries	Accorde l'autorisation d'obtenir les récapitulatifs des recommandations pour le ou les comptes spécifiés	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutRecommendationPreferences	Accorde l'autorisation de définir des préférences de recommandation.	Écrire		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
UpdateEnrollmentStatus	Accorde l'autorisation de mettre à jour le statut d'inscription	Écrire			

Types de ressources définis par AWS Compute Optimizer

AWS Compute Optimizer ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Compute Optimizer, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Compute Optimizer

AWS Compute Optimizer définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
compute-optimizer:ResourceType	Filtre l'accès en fonction du type de ressource	String

Actions, ressources et clés de condition pour AWS Compute Optimizer Automation

AWS Compute Optimizer Automation (préfixe de service :`aco-automation`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Compute Optimizer Automation

- Types de ressources définis par AWS Compute Optimizer Automation
- Clés de condition pour AWS Compute Optimizer Automation

Actions définies par AWS Compute Optimizer Automation

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAccounts	Accorde l'autorisation d'associer les comptes des membres au compte de gestion	Écrire			
CreateAutomationRule	Accorde l'autorisation de créer une règle d'automatisation	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutomationRule	Autorise la suppression de la règle d'automatisation	Écrire	AutomationRule*	aws:ResourceTag/${TagKey}	
DisassociateAccounts	Accorde l'autorisation de dissocier les comptes membres du compte de gestion	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAutomationEvent	Accorde l'autorisation d'obtenir les détails des événements d'automatisation	Lecture			
GetAutomationRule	Accorde l'autorisation d'obtenir une règle d'automatisation	Lecture	AutomationRule*	aws:ResourceTag/${TagKey}	
GetEnrollmentConfiguration	Accorde l'autorisation d'obtenir la configuration d'inscription	Lecture			
ListAccounts	Autorise votre organisation à répertorier les comptes inscrits à Compute Optimizer et à indiquer s'ils ont activé la fonctionnalité d'automatisation	List			
ListAutomationEventSteps	Accorde l'autorisation de répertorier les étapes des événements d'automatisation	List			
ListAutomationEventSummaries	Accorde l'autorisation de répertorier les résumés des événements d'automatisation	List			
ListAutomationEvents	Accorde l'autorisation de répertorier les événements d'automatisation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAutomationRulePreview	Accorde l'autorisation de répertorier les résultats d'aperçu des règles d'automatisation	List			ec2:DescribeVolumes
ListAutomationRulePreviewSummaries	Accorde l'autorisation de répertorier les résumés d'aperçu des règles d'automatisation	List			
ListAutomationRules	Accorde l'autorisation de répertorier les règles d'automatisation	List			
ListRecommendedActionSummaries	Accorde l'autorisation de répertorier les résumés des actions recommandées	List			
ListRecommendedActions	Accorde l'autorisation de répertorier les actions recommandées	List			ec2:DescribeVolumes
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour la règle d'automatisation	List	AutomationRule*	aws:ResourceTag/${TagKey}	
RollbackAutomationEvent	Accorde l'autorisation de lancer une annulation pour un événement d'automatisation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartAutomationEvent	Autorise le lancement d'une automatisation à la demande pour une action recommandée	Écrire			
TagResource	Accorde l'autorisation d'ajouter des balises à la règle d'automatisation	Identification	AutomationRule*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises de la règle d'automatisation	Identification	AutomationRule*	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateAutomationRule	Autorise la mise à jour de la règle d'automatisation	Écrire	AutomationRule*	aws:ResourceTag/${TagKey}	
UpdateEnrollmentConfiguration	Autorise la mise à jour de la configuration d'inscription pour la fonctionnalité d'automatisation de Compute Optimizer	Écrire			

Types de ressources définis par AWS Compute Optimizer Automation

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AutomationRule	`arn:${Partition}:compute-optimizer::${Account}:automation-rule/${RuleId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Compute Optimizer Automation

AWS Compute Optimizer Automation définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Config

AWS Config (préfixe de service :`config`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Config
- Types de ressources définis par AWS Config
- Clés de condition pour AWS Config

Actions définies par AWS Config

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateResourceTypes	Accorde l'autorisation d'ajouter tous les types de ressources spécifiés à l'enregistreur RecordingGroup de configuration et inclut ces types de ressources lors de l'enregistrement	Écrire	ConfigurationRecorder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetAggregateResourceConfig	Accorde l'autorisation de renvoyer les éléments de configuration actuels pour les ressources présentes dans votre agrégateur AWS Config	Lecture	ConfigurationAggregator*		
BatchGetResourceConfig	Accorde l'autorisation de renvoyer la configuration actuelle pour une ou plusieurs ressources demandées	Lecture			
DeleteAggregationAuthorization	Accorde l'autorisation de supprimer l'autorisation accordée au compte agrégateur de la configuration spécifiée dans une région spécifiée	Écrire	AggregationAuthorization*		
DeleteConfigRule	Accorde l'autorisation de supprimer la règle AWS Config spécifiée et tous ses résultats d'évaluation	Écrire	ConfigRule*		
DeleteConfigurationAggregator	Accorde l'autorisation de supprimer l'agrégateur de la configuration spécifiée et les données agrégées associées à l'agrégateur	Écrire	ConfigurationAggregator*		
DeleteConfigurationRecorder	Autorise la suppression de l'enregistreur de configuration géré par le client	Écrire	ConfigurationRecorder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConformancePack	Accorde l'autorisation de supprimer le pack de conformité spécifié, toutes les règles de AWS configuration et tous les résultats d'évaluation contenus dans ce pack de conformité	Écrire	ConformancePack*		
DeleteDeliveryChannel	Accorde l'autorisation de supprimer le canal de livraison	Écriture			
DeleteEvaluationResults	Accorde l'autorisation de supprimer les résultats de l'évaluation pour la règle Config spécifiée	Écriture	ConfigRule*		
DeleteOrganizationConfigRule	Accorde l'autorisation de supprimer la règle Config de l'organisation spécifiée et tous ses résultats d'évaluation de tous les comptes de membres de cette organisation	Écriture	OrganizationConfigRule*		
DeleteOrganizationConformancePack	Accorde l'autorisation de supprimer le pack de conformité de l'organisation spécifié et tous ses résultats d'évaluation de tous les comptes membres de cette organisation	Écriture	OrganizationConformancePack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePendingAggregationRequest	Accorde l'autorisation de supprimer les demandes d'autorisation en attente pour un compte agrégateur spécifié d'une région spécifiée	Écriture			
DeleteRemediationConfiguration	Accorde l'autorisation de supprimer la configuration de la correction	Écrire	RemediationConfiguration*		
DeleteRemediationExceptions	Accorde l'autorisation de supprimer une ou plusieurs exceptions de correction pour des clés de ressource spécifiques pour une règle de AWS configuration spécifique	Écrire			
DeleteResourceConfig	Accorde l'autorisation d'enregistrer l'état de configuration d'une ressource personnalisée qui a été supprimée	Écriture			
DeleteRetentionConfiguration	Accorde l'autorisation de supprimer la configuration de conservation	Écrire			
DeleteServiceLinkedConfigurationRecorder	Accorde l'autorisation de supprimer l'enregistreur de configuration lié au service	Écrire	ConfigurationRecorder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				config:ConfigurationRecorderServicePrincipal	
DeleteStoredQuery	Accorde l'autorisation de supprimer la requête stockée pour un Compte AWS Région AWS	Écrire	StoredQuery*		
DeliverConfigSnapshot	Accorde l'autorisation de planifier la livraison d'un instantané de configuration au compartiment Amazon S3 dans le canal de livraison spécifié	Lecture			
DescribeAggregateComplianceByConfigRules	Accorde l'autorisation de renvoyer la liste des règles conformes et non conformes avec le nombre de ressources pour les règles conformes et non conformes	Lecture	ConfigurationAggregator*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAggregateComplianceByConformancePacks	Accorde l'autorisation de renvoyer une liste de packs de conformité conformes et non conformes, ainsi que le nombre de règles conformes, non conformes et totales dans chaque pack de conformité.	Lecture	ConfigurationAggregator*		
DescribeAggregationAuthorizations	Accorde l'autorisation de renvoyer la liste des autorisations accordées à divers comptes et régions agrégateurs	List			
DescribeComplianceByConfigRule	Accorde l'autorisation d'indiquer si les règles de AWS configuration spécifiées sont conformes	Lecture			
DescribeComplianceByResource	Accorde l'autorisation d'indiquer si les AWS ressources spécifiées sont conformes	Lecture			
DescribeConfigRuleEvaluationStatus	Accorde l'autorisation de renvoyer des informations d'état pour chacune de vos règles de configuration AWS gérées	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeConfigRules	Accorde l'autorisation de renvoyer des informations sur vos règles de AWS Config	List			
DescribeConfigurationAggregatorSourcesStatus	Accorde l'autorisation de renvoyer des informations d'état pour les sources au sein d'un agrégateur	Lecture	ConfigurationAggregator*		
DescribeConfigurationAggregators	Accorde l'autorisation de renvoyer les détails d'un ou plusieurs agrégateurs de configuration	Liste			
DescribeConfigurationRecorderStatus	Accorde l'autorisation de renvoyer l'état actuel de l'enregistreur de configuration spécifié	Lecture	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConfigurationRecorders	Accorde l'autorisation de renvoyer les noms d'un ou de plusieurs enregistreurs de configuration spécifiés	Lecture	ConfigurationRecorder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				config:ConfigurationRecorderServicePrincipal	
DescribeConformancePackCompliance	Accorde l'autorisation de renvoyer les informations de conformité pour chaque règle de ce pack de conformité	Lecture	ConformancePack*		
DescribeConformancePackStatus	Accorde l'autorisation de fournir un ou plusieurs états de déploiement des packs de conformité	Lecture			
DescribeConformancePacks	Accorde l'autorisation de renvoyer la liste d'un ou plusieurs packs de conformité	Liste			
DescribeDeliveryChannelStatus	Accorde l'autorisation de renvoyer l'état actuel du canal de livraison spécifié	Lecture			
DescribeDeliveryChannels	Accorde l'autorisation de renvoyer des détails sur le canal de livraison spécifié	Liste			
DescribeOrganizationConfigRuleStatuses	Accorde l'autorisation de fournir l'état du déploiement des règles Config d'une organisation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeOrganizationConfigRules	Accorde l'autorisation de renvoyer la liste des règles Config d'une organisation	Liste			
DescribeOrganizationConformancePackStatuses	Accorde l'autorisation de fournir l'état du déploiement du pack de conformité d'une organisation	Lecture			
DescribeOrganizationConformancePacks	Accorde l'autorisation de renvoyer la liste de packs de conformité d'une organisation	Liste			
DescribePendingAggregationRequests	Accorde l'autorisation de renvoyer la liste de toutes les demandes d'agrégation en attente	Liste			
DescribeRemediationConfigurations	Accorde l'autorisation de renvoyer les détails d'une ou plusieurs configurations de correction	Liste	RemediationConfiguration*		
DescribeRemediationExceptions	Accorde l'autorisation de renvoyer les détails d'une ou plusieurs exceptions de correction	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRemediationExecutionStatus	Accorde l'autorisation de fournir une vue détaillée de l'exécution d'une correction pour un ensemble de ressources, y compris le statut, les horodatages et les messages d'erreur pour les étapes ayant échoué	Lecture	RemediationConfiguration*		
DescribeRetentionConfigurations	Accorde l'autorisation de renvoyer les détails d'une ou plusieurs configurations de conservation	List			
DisassociateResourceTypes	Accorde l'autorisation de supprimer tous les types de ressources spécifiés de l'enregistreur RecordingGroup de configuration et exclut ces types de ressources lors de l'enregistrement	Écrire	ConfigurationRecorder*		
GetAggregateComplianceDetailsByConfigRule	Accorde l'autorisation de renvoyer les résultats d'évaluation pour la règle AWS Config spécifiée pour une ressource spécifique dans une règle	Lecture	ConfigurationAggregator*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAggregateConfigRuleComplianceSummary	Accorde l'autorisation de renvoyer le nombre de règles conformes et non conformes pour un ou plusieurs comptes et régions d'un agrégateur	Lecture	ConfigurationAggregator*		
GetAggregateConformancePackComplianceSummary	Accorde l'autorisation de renvoyer le nombre de packs de conformité conformes et non conformes pour un ou plusieurs comptes et régions d'un agrégateur.	Lecture	ConfigurationAggregator*		
GetAggregateDiscoveredResourceCounts	Accorde l'autorisation de renvoyer le nombre de ressources pour les comptes et les régions présents dans votre agrégateur AWS Config	Lecture	ConfigurationAggregator*		
GetAggregateResourceConfig	Accorde l'autorisation de renvoyer l'élément de configuration qui est agrégé pour votre ressource spécifique dans un compte et une région source spécifiques	Lecture	ConfigurationAggregator*		
GetComplianceDetailsByConfigRule	Accorde l'autorisation de renvoyer les résultats d'évaluation pour la règle AWS Config spécifiée	Lecture	ConfigRule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetComplianceDetailsByResource	Accorde l'autorisation de renvoyer les résultats de l'évaluation pour la AWS ressource spécifiée	Lecture			
GetComplianceSummaryByConfigRule	Accorde l'autorisation de renvoyer le nombre de règles AWS Config conformes et non conformes, jusqu'à un maximum de 25 pour chacune	Lecture			
GetComplianceSummaryByResourceType	Accorde l'autorisation de renvoyer le nombre de ressources qui sont conformes et le nombre de ressources qui sont non conformes	Lecture			
GetConformancePackComplianceDetails	Accorde l'autorisation de renvoyer les informations de conformité d'un pack de conformité pour toutes les AWS ressources surveillées par le pack de conformité	Lecture	ConformancePack*		
GetConformancePackComplianceSummary	Accorde l'autorisation de fournir un résumé de la conformité pour un ou plusieurs packs de conformité	Lecture	ConformancePack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCustomRulePolicy	Accorde l'autorisation de renvoyer la définition de politique contenant la logique de votre règle AWS Config Custom Policy	Lecture	ConfigRule*		
GetDiscoveredResourceCounts	Accorde l'autorisation de renvoyer les types de ressources, le nombre de chaque type de ressource et le nombre total de ressources que AWS Config enregistre dans cette région pour votre Compte AWS	Lecture			
GetOrganizationConfigRuleDetailedStatus	Accorde l'autorisation de renvoyer le statut détaillé de chaque compte membre au sein d'une organisation pour une règle Config d'organisation donnée	Lecture	OrganizationConfigRule*		
GetOrganizationConformancePackDetailedStatus	Accorde l'autorisation de renvoyer le statut détaillé de chaque compte membre au sein d'une organisation pour un pack de conformité de l'organisation donné	Lecture	OrganizationConformancePack*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOrganizationCustomRulePolicy	Accorde l'autorisation de renvoyer la définition de politique contenant la logique de la règle AWS Config Custom Policy de votre organisation	Lecture	OrganizationConfigRule*		
GetResourceConfigHistory	Accorde l'autorisation de renvoyer la liste d'éléments de configuration pour la ressource spécifiée	Lecture			
GetResourceEvaluationSummary	Accorde l'autorisation de renvoyer le résumé des évaluations des ressources pour un ID d'évaluation de ressources spécifique	Lecture			
GetStoredQuery	Accorde l'autorisation de renvoyer les détails d'une requête stockée spécifique	Lecture	StoredQuery*		
ListAggregateDiscoveredResources	Accorde l'autorisation d'accepter un type de ressource et de renvoyer la liste des identifiants de ressources qui sont regroupés pour un type de ressources spécifique entre les comptes et les régions	List	ConfigurationAggregator*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConfigurationRecorders	Accorde l'autorisation de répertorier les résumés des enregistreurs de configuration pour un Compte AWS dans un Région AWS	List			
ListConformancePackComplianceScores	Accorde l'autorisation de renvoyer le pourcentage de combinaisons règle-ressource conformes dans un pack de conformité par rapport au nombre total de combinaisons règles-ressources possibles	List			
ListDiscoveredResources	Accorde l'autorisation d'accepter un type de ressources et renvoie la liste des identifiants de ressources correspondant aux ressources de ce type	List			
ListResourceEvaluations	Accorde l'autorisation de répertorier les résumés d'évaluation des ressources pour un Compte AWS Région AWS	List			
ListStoredQueries	Accorde l'autorisation de répertorier les requêtes stockées pour un Compte AWS Région AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises de la ressource AWS Config	Lecture	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutAggregationAuthorization	Accorde l'autorisation de permettre au compte agrégateur et la région à collecter les données depuis le compte et la région sources	Écrire	AggregationAuthorization*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigRule	Accorde l'autorisation d'ajouter ou de mettre à jour une règle de AWS configuration pour évaluer si vos AWS ressources sont conformes aux configurations souhaitées	Écrire	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutConfigurationAggregator	Accorde l'autorisation de créer et de mettre à jour l'agrégateur de configuration avec les comptes et régions sources sélectionnés	Écrire	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationRecorder	Accorde l'autorisation de créer ou de mettre à jour un enregistreur de configuration géré par le client pour enregistrer les configurations de ressources sélectionnées	Écrire	ConfigurationRecorder*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutConformancePack	Accorde l'autorisation de créer ou de mettre à jour un pack de conformité	Écriture	ConformancePack*		iam:CreateServiceLinkedRole iam:PassRole s3:GetObject s3:ListBucket ssm:GetDocument
PutDeliveryChannel	Accorde l'autorisation de créer un objet de canal de livraison pour fournir des informations de configuration à un compartiment Amazon S3 et à une rubrique Amazon SNS	Écrire			
PutEvaluations	Accorde l'autorisation d'être utilisée par une fonction AWS Lambda pour fournir des résultats d'évaluation à Config AWS	Écrire			
PutExternalEvaluation	Accorde l'autorisation de fournir le résultat de l'évaluation à AWS Config	Écrire	ConfigRule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutOrganizationConfigRule	Accorde l'autorisation d'ajouter ou de mettre à jour une règle de configuration d'organisation pour l'ensemble de votre organisation en évaluant si vos AWS ressources sont conformes aux configurations souhaitées	Écrire	OrganizationConfigRule*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutOrganizationConformancePack	Accorde l'autorisation d'ajouter ou de mettre à jour le pack de conformité organisationnel pour l'ensemble de votre organisation, en évaluant si vos AWS ressources sont conformes aux configurations souhaitées	Écrire	OrganizationConformancePack*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators s3:GetObject
PutRemediationConfigurations	Accorde l'autorisation d'ajouter ou de mettre à jour la configuration de correction avec une règle de AWS configuration spécifique avec la cible ou l'action sélectionnée	Écrire	RemediationConfiguration*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutRemediationExceptions	Accorde l'autorisation d'ajouter ou de mettre à jour des exceptions de correction pour des ressources spécifiques pour une règle de AWS configuration spécifique	Écrire			
PutResourceConfig	Accorde l'autorisation d'enregistrer l'état de configuration pour la ressource fournie dans la demande	Écrire			
PutRetentionConfiguration	Accorde l'autorisation de créer et de mettre à jour la configuration de rétention avec des détails sur la période de rétention (nombre de jours) pendant laquelle AWS Config stocke vos informations historiques	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutServiceLinkedConfigurationRecorder	Accorde l'autorisation de créer un nouvel enregistreur de configuration lié à un service pour enregistrer les configurations de ressources dans le champ d'application du service lié	Écrire		aws:RequestTag/${TagKey} aws:TagKeys config:ConfigurationRecorderServicePrincipal	iam:CreateServiceLinkedRole iam:PassRole
PutStoredQuery	Accorde l'autorisation d'enregistrer une nouvelle requête ou de mettre à jour une requête enregistrée existante	Écrire	StoredQuery*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SelectAggregateResourceConfig	Accorde l'autorisation d'accepter une commande SELECT en langage de requête structuré (SQL) et un agrégateur pour interroger l'état de configuration des AWS ressources sur plusieurs comptes et régions, effectuer la recherche correspondante et renvoyer les configurations de ressources correspondant aux propriétés	Lecture	ConfigurationAggregator*		
SelectResourceConfig	Accorde l'autorisation d'accepter une commande SELECT SQL, d'effectuer la recherche correspondante, et de renvoyer les configurations de ressources correspondant aux propriétés	Lecture			
StartConfigRulesEvaluation	Accorde l'autorisation d'évaluer vos ressources par rapport aux règles Config spécifiées	Écrire	ConfigRule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartConfigurationRecorder	Autorise l'enregistreur de configuration géré par le client à commencer à enregistrer les configurations des AWS ressources que vous avez sélectionnées pour enregistrer dans votre Compte AWS	Écrire	ConfigurationRecorder*		
StartRemediationExecution	Autorise l'exécution d'une correction à la demande pour les règles de AWS configuration spécifiées par rapport à la dernière configuration de correction connue	Écrire			iam:PassRole
StartResourceEvaluation	Accorde l'autorisation d'évaluer les détails de vos ressources par rapport aux règles AWS Config de votre compte	Écrire			cloudformation:DescribeType
StopConfigurationRecorder	Autorise l'enregistreur de configuration géré par le client à arrêter d'enregistrer les configurations AWS des ressources que vous avez sélectionnées pour enregistrer dans votre Compte AWS	Écrire	ConfigurationRecorder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'associer les balises spécifiées à une ressource avec le resourceArn spécifié	Balisage	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées d'une ressource	Identification	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			StoredQuery		
				aws:TagKeys	

Types de ressources définis par AWS Config

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AggregationAuthorization	`arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}`	aws:ResourceTag/${TagKey}
ConfigurationAggregator	`arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}`	aws:ResourceTag/${TagKey}
ConfigRule	`arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
ConformancePack	arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}	aws:ResourceTag/${TagKey}
OrganizationConfigRule	arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}	aws:ResourceTag/${TagKey}
OrganizationConformancePack	arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}	aws:ResourceTag/${TagKey}
RemediationConfiguration	arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}	
StoredQuery	arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}	aws:ResourceTag/${TagKey}
ConfigurationRecorder	arn:${Partition}:config:${Region}:${Account}:configuration-recorder/${RecorderName}/${RecorderId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Config

AWS Config définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString
config:ConfigurationRecorderServicePrincipal	Filtre l'accès par service principal de l'enregistreur de configuration	String

Actions, ressources et clés de condition pour Amazon Connect Cases

Amazon Connect Cases (préfixe de service : `cases`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Connect Cases
- Types de ressources définis par Amazon Connect Cases
- Clés de condition pour Amazon Connect Cases

Actions définies par Amazon Connect Cases

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetCaseRule	Accorde l'autorisation de récupérer des informations sur les règles du dossier dans le domaine du dossier	Lecture	CaseRule*		
			Domain*		
BatchGetField	Accorde l'autorisation de récupérer des informations sur les champs dans le domaine du cas	Lecture	Domain*		
			Field*		
BatchPutFieldOptions	Accorde l'autorisation de mettre à jour les options du champ dans le domaine du cas	Écrire	Domain*		
			Field*		
CreateCase	Accorde l'autorisation de créer un cas dans le domaine du cas	Écrire	Case*		
			Domain*		
			Field*		
			Template*		
				connect:UserArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCaseRule	Accorde l'autorisation de créer une règle de cas dans le domaine de cas	Écrire	CaseRule*		
			Domain*		
CreateDomain	Accorde l'autorisation de créer un domaine du cas	Écrire			
CreateField	Accorde l'autorisation de créer un champ dans le domaine du cas	Écrire	Domain*		
			Field*		
CreateLayout	Accorde l'autorisation de créer une disposition dans le domaine du cas	Écrire	Domain*		
			Layout*		
CreateRelatedItem	Accorde l'autorisation de créer un élément associé à un cas dans le domaine du cas	Écrire	Case*		
			Domain*		
			RelatedItem*		
				connect:UserArn	
CreateTemplate	Accorde l'autorisation de créer un modèle dans le domaine du cas	Écrire	Domain*		
			Layout*		
			Template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCase	Accorde l'autorisation de supprimer le dossier dans le domaine du dossier	Écrire	Case*		
			Domain*		
DeleteCaseRule	Accorde l'autorisation de supprimer la règle de cas dans le domaine de cas	Écrire	CaseRule*		
			Domain*		
DeleteDomain	Octroie l'autorisation de supprimer le domaine	Écrire	Domain*		
DeleteField	Accorde l'autorisation de supprimer le champ dans le domaine de dossier	Écrire	Domain*		
			Field*		
DeleteLayout	Accorde l'autorisation de supprimer la mise en page dans le domaine case	Écrire	Domain*		
			Layout*		
DeleteRelatedItem	Accorde l'autorisation de supprimer l'élément associé au dossier dans le domaine du dossier	Écrire	Case*		
			Domain*		
			RelatedItem*		
DeleteTemplate	Accorde l'autorisation de supprimer le modèle dans le domaine de dossier	Écrire	Domain*		
			Template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCase	Accorde l'autorisation de récupérer des informations sur un cas dans le domaine du cas	Lecture	Case*		
			Domain*		
			Field*		
GetCaseAuditEvents	Autorise l'accès à l'historique d'audit d'un dossier	Lecture	Case*		
			Domain*		
GetCaseEventConfiguration	Accorde l'autorisation de récupérer des informations sur la configuration d'un événement du cas dans le domaine du cas	Lecture	Domain*		
GetDomain	Accorde l'autorisation de récupérer des informations sur le domaine du cas	Lecture	Domain*		
GetLayout	Accorde l'autorisation de récupérer des informations sur la disposition dans le domaine du cas	Lecture	Domain*		
			Layout*		
GetTemplate	Accorde l'autorisation de récupérer des informations sur le modèle dans le domaine du cas	Lecture	Domain*		
			Template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCaseRules	Accorde l'autorisation de répertorier les règles du dossier dans le domaine du dossier	List	Domain*		
ListCasesForContact	Accorde l'autorisation de répertorier les cas pour un contact spécifique dans le domaine du cas	List	Domain*		
ListDomains	Accorde l'autorisation de répertorier tous les domaines dans le compte aws	List			
ListFieldOptions	Accorde l'autorisation de répertorier les options de champ pour un champ unique sélectionné dans le domaine du cas	List	Domain* Field*		
ListFields	Accorde l'autorisation de répertorier les champs dans le domaine du cas	List	Domain*		
ListLayouts	Accorde l'autorisation de répertorier les dispositions dans le domaine du cas	List	Domain*		
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTemplates	Accorde l'autorisation de répertorier les modèles dans le domaine du cas	List	Domain*		
PutCaseEventConfiguration	Accorde l'autorisation d'insérer ou de mettre à jour la configuration de l'événement du cas dans le domaine du cas	Écrire	Domain*		
SearchCases	Accorde l'autorisation de rechercher des cas dans le domaine du cas	Lecture	Domain*		
SearchRelatedItems	Accorde l'autorisation de rechercher les éléments associés à un cas dans le domaine du cas	Lecture	Case*		
			Domain*		
TagResource	Accorde l'autorisation d'ajouter les balises spécifiées à la ressource spécifiée	Identification	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de la ressource spécifiée	Identification	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		
				aws:TagKeys	
UpdateCase	Accorde l'autorisation de mettre à jour les valeurs de champ du cas dans le domaine du cas	Écrire	Case*		
			Domain*		
			Field*		
				connect:UserArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCaseRule	Accorde l'autorisation de mettre à jour la règle du dossier dans le domaine du dossier	Écrire	CaseRule* Domain*		
UpdateField	Accorde l'autorisation de mettre à jour un champ dans le domaine du cas	Écrire	Domain* Field*		
UpdateLayout	Accorde l'autorisation de mettre à jour la disposition dans le domaine du cas	Écrire	Domain* Layout*		
UpdateTemplate	Accorde l'autorisation de mettre à jour le modèle dans le domaine du cas	Écrire	Domain* Template*		

Types de ressources définis par Amazon Connect Cases

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Case	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}	aws:ResourceTag/${TagKey}
Domain	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}	aws:ResourceTag/${TagKey}
Field	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/field/${FieldId}	aws:ResourceTag/${TagKey}
Layout	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/layout/${LayoutId}	aws:ResourceTag/${TagKey}
RelatedItem	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}/related-item/${RelatedItemId}	aws:ResourceTag/${TagKey}
Template	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/template/${TemplateId}	aws:ResourceTag/${TagKey}
CaseRule	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case-rule/${CaseRuleId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Connect Cases

Amazon Connect Cases définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString
connect:UserArn	Filtre l'accès par connexion UserArn	ARN

Actions, ressources et clés de condition pour Amazon Connect Customer Profiles

Amazon Connect Customer Profiles (préfixe de service : `profile`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Connect Customer Profiles
- Types de ressources définis par Amazon Connect Customer Profiles
- Clés de condition pour Amazon Connect Customer Profiles

Actions définies par Amazon Connect Customer Profiles

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddProfileKey	Accorde l'autorisation d'ajouter une clé de profil.	Écrire	domains*		
BatchGetCalculatedAttributeForProfile	Accorde l'autorisation de récupérer un attribut calculé pour les profils spécifiques du domaine	Lecture	calculated-attributes*		
			domains*		
BatchGetProfile	Accorde l'autorisation d'obtenir des profils dans le domaine	Lecture	domains*		
CreateCalculatedAttributeDefinition	Accorde l'autorisation de créer une définition d'attribut calculé dans le domaine	Écrire	calculated-attributes*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		
CreateDomain	Accorde l'autorisation de créer un domaine.	Écrire	domains*	aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateDomainLayout	Accorde l'autorisation de créer une mise en page dans le domaine	Écrire	domains*		
			layouts*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventStream	Accorde l'autorisation de placer un flux d'événements dans un domaine	Écrire	domains*		iam:PutRolePolicy kinesis:DescribeStreamSummary
			event-streams*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventTrigger	Accorde l'autorisation de créer un déclencheur d'événement dans le domaine	Écrire	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			event-triggers*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationWorkflow	Accorde l'autorisation de créer un flux d'intégration dans un domaine	Écrire	domains*		
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Accorde l'autorisation de créer un profil dans le domaine.	Écrire	domains*		
CreateRecommender	Accorde l'autorisation de créer un recommendeur dans le domaine	Écrire	domains*		
			recommenders*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSegmentDefinition	Accorde l'autorisation de créer une définition de segment dans le domaine	Écrire	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			segment-definitions*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSegmentEstimate	Autorise la création d'une estimation de segment dans le domaine	Écrire	domains*		
CreateSegmentSnapshot	Accorde l'autorisation de créer un instantané de segment dans le domaine	Écrire	domains*		
			segment-definitions*		
CreateSnapshot [autorisation uniquement]	Accorde l'autorisation de créer un instantané dans le domaine	Écrire	domains*		
CreateUploadJob	Accorde l'autorisation de créer une tâche de téléchargement dans le domaine	Écrire	domains*		
DeleteCalculatedAttributeDefinition	Accorde l'autorisation de supprimer une définition d'attribut calculé dans le domaine	Écrire	calculated-attributes*		
			domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDomain	Accorde l'autorisation de supprimer un domaine	Écrire	domains*		
DeleteDomainLayout	Accorde l'autorisation de supprimer une mise en page dans le domaine	Écrire	domains*		
			layouts*		
DeleteDomainObjectType	Accorde l'autorisation de supprimer un type d'objet de domaine spécifique dans le domaine	Écrire	domain-object-types*		
			domains*		
DeleteEventStream	Accorde l'autorisation de supprimer un flux d'événements dans un domaine	Écrire	domains*		iam:DeleteRolePolicy
			event-streams*		
DeleteEventTrigger	Accorde l'autorisation de supprimer un déclencheur d'événement dans le domaine	Écrire	domains*		
			event-triggers*		
DeleteIntegration	Accorde l'autorisation de supprimer une intégration dans un domaine.	Écriture	domains*		
			integrations*		
DeleteProfile	Accorde l'autorisation de supprimer un profil.	Écriture	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteProfileKey	Accorde l'autorisation de supprimer une clé de profil.	Écriture	domains*		
DeleteProfileObject	Accorde l'autorisation de supprimer un objet de profil.	Écriture	domains*		
			object-types*		
DeleteProfileObjectType	Accorde l'autorisation de supprimer un type d'objet de profil spécifique dans le domaine.	Écrire	domains*		
			object-types*		
DeleteRecommender	Autorise la suppression d'un recommandeur dans un domaine	Écrire	domains*		
			recommenders*		
DeleteSegmentDefinition	Autorise la suppression d'une définition de segment dans le domaine	Écrire	domains*		
			segment-definitions*		
DeleteWorkflow	Accorde l'autorisation de supprimer un flux de travail dans un domaine	Écrire	domains*		
DetectProfileObjectType	Octroie l'autorisation de détecter automatiquement le type d'objet.	Lecture	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAutoMergingPreview	Accorde l'autorisation d'obtenir une prévisualisation de la fusion automatique dans un domaine	Lecture	domains*		
GetCalculatedAttributeDefinition	Accorde l'autorisation d'obtenir une définition d'attribut calculé dans le domaine	Lecture	calculated-attributes*		
			domains*		
GetCalculatedAttributeForProfile	Accorde l'autorisation de récupérer un attribut calculé pour un profil spécifique dans le domaine	Lecture	calculated-attributes*		
			domains*		
GetDomain	Accorde l'autorisation d'obtenir un domaine spécifique dans un compte	Lecture	domains*		
GetDomainLayout	Accorde l'autorisation d'obtenir une mise en page dans le domaine	Lecture	domains*		
			layouts*		
GetDomainObjectType	Accorde l'autorisation d'obtenir un type d'objet de domaine spécifique dans le domaine	Lecture	domain-object-types*		
			domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEventStream	Accorde l'autorisation d'obtenir un flux d'événements spécifique dans un domaine	Lecture	domains*		kinesis:DescribeStreamSummary
			event-streams*		
GetEventTrigger	Accorde l'autorisation d'obtenir un déclencheur d'événement dans le domaine	Lecture	domains*		
			event-triggers*		
GetIdentityResolutionJob	Accorde l'autorisation d'obtenir une tâche de résolution d'identité dans un domaine	Lecture	domains*		
GetIntegration	Accorde l'autorisation d'obtenir une intégration spécifique dans un domaine.	Lecture	domains*		
			integrations*		
GetMatches	Accorde l'autorisation d'obtenir des correspondances de profil dans un domaine	List	domains*		
GetObjectTypeAttributeStatistics	Accorde l'autorisation d'obtenir les statistiques d'un attribut spécifique pour un type d'objet dans le domaine	Lecture	domains*		
			object-types*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProfileHistoryRecord	Accorde l'autorisation d'obtenir un enregistrement d'historique de profil pour un profil dans un domaine	Lecture	domains*		
GetProfileInsights	Accorde l'autorisation de répertorier les informations d'un profil	Lecture	domains*		
GetProfileObjectType	Accorde l'autorisation d'obtenir un type d'objet de profil spécifique dans le domaine.	Lecture	domains*		
			object-types*		
GetProfileObjectTypeTemplate	Accorde l'autorisation d'obtenir un modèle de type d'objet spécifique.	Lecture			
GetProfileRecommendations	Accorde l'autorisation de répertorier les recommandations pour un profil	Lecture	domains*		
			recommenders*		
GetRecommender	Accorde l'autorisation d'obtenir les détails du recommandeur dans un domaine	Lecture	domains*		
			recommenders*		
GetSegmentDefinition	Accorde l'autorisation d'obtenir une définition de segment dans le domaine	Lecture	domains*		
			segment-definitions*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSegmentEstimate	Accorde l'autorisation d'obtenir une estimation du segment dans le domaine	Lecture	domains*		
GetSegmentMembership	Accorde l'autorisation de déterminer si les profils donnés font partie d'un segment du domaine	Lecture	domains*		
			segment-definitions*		
GetSegmentSnapshot	Accorde l'autorisation d'obtenir un instantané du segment dans le domaine	Lecture	domains*		
			segment-definitions*		
GetSimilarProfiles	Octroie l'autorisation d'obtenir tous les profils similaires du domaine.	List	domains*		
GetSnapshot [autorisation uniquement]	Accorde l'autorisation d'obtenir un instantané dans le domaine	Lecture	domains*		
GetUploadJob	Accorde l'autorisation d'obtenir les détails d'une tâche de téléchargement dans le domaine	Lecture	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetUploadJobPath	Accorde l'autorisation d'obtenir une URL pré-signée pour télécharger un fichier dans le cadre d'une tâche de téléchargement	Lecture	domains*		
GetWorkflow	Accorde l'autorisation d'obtenir les détails d'un flux de travail dans un domaine	Lecture	domains*		
GetWorkflowSteps	Accorde l'autorisation d'obtenir les détails des étapes de flux de travail dans un domaine	Lecture	domains*		
ListAccountIntegrations	Accorde l'autorisation de créer la liste de toutes les intégrations dans le compte.	List			
ListCalculatedAttributeDefinitions	Accorde l'autorisation de répertorier toutes les définitions d'attributs calculés dans le domaine	List	domains*		
ListCalculatedAttributesForProfile	Accorde l'autorisation de répertorier tous les attributs calculés pour un profil spécifique dans le domaine	List	domains*		
ListDomainLayouts	Accorde l'autorisation de répertorier toutes les mises en page du domaine	List	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDomainObjectTypes	Accorde l'autorisation de répertorier tous les types d'objets du domaine	List	domains*		
ListDomainObjects	Accorde l'autorisation de répertorier des objets de domaine dans un domaine	List	domain-object-types*		
			domains*		
ListDomains	Accorde l'autorisation de répertorier tous les domaines d'un compte.	List			
ListEventStreams	Accorde l'autorisation de répertorier tous les flux d'événements dans un domaine spécifique	List	domains*		
ListEventTriggers	Accorde l'autorisation de répertorier tous les déclencheurs d'événements du domaine	List	domains*		
ListIdentityResolutionJobs	Accorde l'autorisation de répertorier les tâches de résolution d'identité dans un domaine	List	domains*		
ListIntegrations	Accorde l'autorisation de répertorier toutes les intégrations dans un domaine spécifique.	List	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListObjectTypeAttributeValues	Accorde l'autorisation de répertorier les valeurs d'un attribut spécifique pour un type d'objet dans le domaine	List	domains* object-types*		
ListObjectTypeAttributes	Accorde l'autorisation de répertorier tous les attributs d'un type d'objet spécifique dans le domaine	List	domains* object-types*		
ListProfileAttributeValues	Accorde l'autorisation de répertorier toutes les valeurs d'un attribut de profil dans le domaine	List	domains*		
ListProfileHistoryRecords	Accorde l'autorisation de répertorier tous les enregistrements d'historique de profil pour un profil dans un domaine	List	domains*		
ListProfileObjectTypeTemplates	Accorde l'autorisation de répertorier tous les modèles de type d'objet de profil dans le compte.	Liste			
ListProfileObjectTypes	Accorde l'autorisation de répertorier tous les types d'objets de profil dans le domaine.	Liste	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProfileObjects	Accorde l'autorisation de répertorier tous les objets de profil pour un profil.	List	domains*		
			object-types*		
ListRecommenderRecipes	Accorde l'autorisation de répertorier toutes les recettes de recommandation du domaine	List			
ListRecommenders	Accorde l'autorisation de répertorier tous les recommandeurs du domaine	List	domains*		
ListRuleBasedMatches	Octroie l'autorisation de répertorier tous les résultats correspondants basés sur des règles dans le domaine.	List	domains*		
ListSegmentDefinitions	Accorde l'autorisation de répertorier toutes les définitions de segments du domaine	List	domains*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	calculated-attributes		
			domain-object-types		
			domains		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			recommenders		
			segment-definitions		
ListUploadJobs	Accorde l'autorisation de répertorier toutes les tâches de téléchargement du domaine	List	domains*		
ListWorkflows	Accorde l'autorisation de répertorier tous les flux de travail dans un domaine spécifique	List	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
MergeProfiles	Accorde l'autorisation de fusionner des profils dans un domaine	Écrire	domains*		
PutDomainObjectType	Accorde l'autorisation de placer un type d'objet de domaine spécifique dans le domaine	Écrire	domain-object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutIntegration	Accorde l'autorisation de placer une intégration dans un domaine	Écriture	domains*		app-integrations:CreateDataIntegrationAssociation app-integrations:DeleteDataIntegrationAssociation app-integrations:GetDataIntegration app-integrations:ListDataIntegrationAssociations kms:CreateGrant

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
PutProfileObject	Accorde l'autorisation de placer un objet pour un profil.	Écriture	domains*		
			object-types*		
PutProfileObjectType	Accorde l'autorisation de placer un type d'objet de profil spécifique dans le domaine.	Écriture	domains*		
			object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
SearchProfiles	Accorde l'autorisation de rechercher des profils dans un domaine.	Lecture	domains*		
StartRecommender	Autorise le lancement d'un recommandeur dans un domaine	Écrire	domains*		
			recommenders*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartUploadJob	Accorde l'autorisation de démarrer une tâche de téléchargement dans le domaine	Écrire	domains*		
StopRecommender	Accorde l'autorisation d'arrêter un recommandeur dans un domaine	Écrire	domains*		
			recommenders*		
StopUploadJob	Accorde l'autorisation d'arrêter une tâche de téléchargement dans le domaine	Écrire	domains*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	calculated-attributes		
			domain-object-types		
			domains		
			event-streams		
			event-triggers		
			integrations		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			layouts		
			object-types		
			recommenders		
			segment-definitions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	calculated-attributes		
			domain-object-types		
			domains		
			event-streams		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			event-triggers		
			integrations		
			layouts		
			object-types		
			recommenders		
			segment-definitions		
				aws:TagKeys	
UpdateCalculatedAttributeDefinition	Accorde l'autorisation de mettre à jour d'une définition d'attribut calculé dans le domaine	Écrire	calculated-attributes*		
			domains*		
UpdateDomain	Accorde l'autorisation de mettre à jour un domaine	Écrire	domains*		iam:CreateServiceLinkedRole
UpdateDomainLayout		Écrire	domains*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de mettre à jour une mise en page dans le domaine		layouts*		
UpdateEventTrigger	Autorise la mise à jour d'un déclencheur d'événement dans le domaine	Écrire	domains*		
			event-triggers*		
UpdateProfile	Accorde l'autorisation de mettre à jour un profil dans le domaine.	Écrire	domains*		
UpdateRecommender	Autorise la mise à jour d'un recommendeur dans le domaine	Écrire	domains*		
			recommenders*		

Types de ressources définis par Amazon Connect Customer Profiles

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
domains	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
object-types	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/object-types/${ObjectTypeName}	aws:ResourceTag/${TagKey}
integrations	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/integrations/${Uri}	aws:ResourceTag/${TagKey}
event-streams	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-streams/${EventStreamName}	aws:ResourceTag/${TagKey}
calculated-attributes	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/calculated-attributes/${CalculatedAttributeName}	aws:ResourceTag/${TagKey}
segment-definitions	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/segment-definitions/${SegmentDefinitionName}	aws:ResourceTag/${TagKey}
event-triggers	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-triggers/${EventTriggerName}	aws:ResourceTag/${TagKey}
layouts	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/layouts/${LayoutDefinitionName}	aws:ResourceTag/${TagKey}
recommenders	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/recommenders/${RecommenderTypeName}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
domain-object-types	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/domain-object-types/${ObjectTypeName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Connect Customer Profiles

Amazon Connect Customer Profiles définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'une clé qui est présente dans la demande envoyée par l'utilisateur au service de profil client	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction d'une paire de clé et de valeur de balise	String
aws:TagKeys	Filtre l'accès en fonction de la liste de tous les noms de clé de balise présents dans la demande envoyée par l'utilisateur au service de profil client	ArrayOfString

Actions, ressources et clés de condition pour Amazon Connect Health

Amazon Connect Health (préfixe de service :`health-agent`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Connect Health
- Types de ressources définis par Amazon Connect Health
- Clés de condition pour Amazon Connect Health

Actions définies par Amazon Connect Health

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateSubscription	Accorde l'autorisation d'activer un abonnement pour permettre la facturation pour un utilisateur	Écrire	Domain*		
			Subscription*		
CancelAppointment [autorisation uniquement]	Autorise l'annulation d'un rendez-vous	Écrire	Domain*		
			Integration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAgent [autorisation uniquement]	Accorde l'autorisation de créer un nouvel agent avec une version initiale à l'état DRAFT	Écrire	Agent*		
			Domain*		
CreateDomain	Accorde l'autorisation de créer un nouveau domaine pour gérer les HealthAgent ressources	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	health-agent:TagResource iam:PassRole
CreateIntegration [autorisation uniquement]	Accorde l'autorisation de créer une nouvelle intégration pour un domaine	Écrire	Domain*		
			Integration*		
CreateSession [autorisation uniquement]	Accorde l'autorisation de créer une nouvelle session avec des configurations d'agent spécifiées	Écrire	Agent*		
			Domain*		
			Session*		
CreateSubscription	Accorde l'autorisation de créer un nouvel abonnement au sein d'un domaine pour la facturation et la gestion des utilisateurs	Écrire	Domain*		
			Subscription*		
DeactivateSubscription	Accorde l'autorisation de désactiver un abonnement pour arrêter la facturation d'un utilisateur	Écrire	Domain*		
			Subscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAgent [autorisation uniquement]	Autorise la suppression d'une configuration d'agent et de toutes ses versions	Écrire	Agent*		
			Domain*		
DeleteDomain	Autorise la suppression d'un domaine et de toutes les ressources associées	Écrire	Domain*		
DeleteIntegration [autorisation uniquement]	Accorde l'autorisation de supprimer une intégration	Écrire	Domain*		
			Integration*		
GetAgent [autorisation uniquement]	Accorde l'autorisation de récupérer la configuration d'un agent, en utilisant par défaut la version la plus récente si elle n'est pas spécifiée	Lecture	Agent*		
			Domain*		
GetCareTeamProvider [autorisation uniquement]	Donne l'autorisation de récupérer le fournisseur de soins d'un patient	Lecture	Domain*		
			Integration*		
GetDomain	Accorde l'autorisation de récupérer des informations sur un domaine	Lecture	Domain*		
GetIntegration [autorisation uniquement]	Accorde l'autorisation d'obtenir une intégration existante	Lecture	Domain*		
			Integration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMedicalScribeListeningSession	Permet de récupérer des informations sur une session d'écoute de Medical Scribe existante	Lecture	Domain*		
			Subscription*		
GetPatient [autorisation uniquement]	Accorde l'autorisation de récupérer les informations du patient	Lecture	Domain*		
			Integration*		
GetPatientInsightsJob	Accorde l'autorisation d'obtenir des informations sur une offre d'information sur les patients entamée	Lecture	Domain*		
			PatientInsightsJob*		
GetPractitioner [autorisation uniquement]	Donne l'autorisation de récupérer les informations du praticien	Lecture	Domain*		
			Integration*		
GetSessionContext [autorisation uniquement]	Accorde l'autorisation de récupérer le contexte de session structuré, y compris les attributs et les données collectées	Lecture	Domain*		
			Session*		
GetSubscription	Accorde l'autorisation de récupérer des informations relatives à un abonnement	Lecture	Domain*		
			Subscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvokeAgent [autorisation uniquement]	Accorde l'autorisation d'invoquer un agent au cours d'une session avec prise en charge des réponses en streaming	Écrire	Domain* Session*		
ListAgents [autorisation uniquement]	Accorde l'autorisation de répertorier tous les agents d'un domaine	List	Domain*		
ListAppointmentSlots [autorisation uniquement]	Accorde l'autorisation de répertorier les créneaux de rendez-vous disponibles	Lecture	Domain* Integration*		
ListDomains	Accorde l'autorisation de répertorier des domaines pour un compte donné	List			
ListIntegrations [autorisation uniquement]	Accorde l'autorisation de répertorier les intégrations pour un domaine	List	Domain*		
ListPatientAppointments [autorisation uniquement]	Donne l'autorisation de répertorier les rendez-vous des patients	Lecture	Domain* Integration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPatientInsuranceCoverages [autorisation uniquement]	Donne l'autorisation de répertorier les couvertures d'assurance pour les patients	Lecture	Domain* Integration*		
ListProviders [autorisation uniquement]	Permet de récupérer les prestataires actifs disponibles pour planifier des rendez-vous avec un patient	Lecture	Domain* Integration*		
ListSubscriptions	Accorde l'autorisation de répertorier tous les abonnements d'un domaine	List	Domain*		
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée	List	Domain		
MatchPatient [autorisation uniquement]	Donne l'autorisation de jumeler un patient	Lecture	Domain* Integration*		
PublishAgent [autorisation uniquement]	Accorde l'autorisation de publier une version de configuration d'agent	Écrire	Agent* Domain*		
RescheduleAppointment [autorisation uniquement]	Autorise le report d'un rendez-vous	Écrire	Domain* Integration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ScheduleAppointment [autorisation uniquement]	Permet de fixer un rendez-vous pour un patient	Écrire	Domain*		
			Integration*		
StartMedicalScribeListeningSession	Autorise le lancement d'une nouvelle session d'écoute de Medical Scribe pour une transcription audio en temps réel	Écrire	Domain*		
			Subscription*		
StartPatientInsightsJob	Accorde l'autorisation de démarrer un nouveau travail d'information sur les patients	Écrire	Domain*		
			PatientInsightsJob*		
TagResource	Accorde l'autorisation d'ajouter les balises spécifiées à la ressource spécifiée	Identification	Domain	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les balises identifiées par la TagKeys liste d'une ressource	Identification	Domain		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgent [autorisation uniquement]	Accorde l'autorisation de mettre à jour un brouillon de configuration d'agent, en créant un nouveau brouillon s'il n'en existe aucun	Écrire	Agent*		
			Domain*		
UpdateIntegration [autorisation uniquement]	Autorise la mise à jour d'une intégration existante	Écrire	Domain*		
			Integration*		
UpdateSession [autorisation uniquement]	Accorde l'autorisation de mettre à jour les attributs de session tels que DepartmentID et AppointmentType	Écrire	Domain*		
			Session*		

Types de ressources définis par Amazon Connect Health

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Domain	`arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
PatientInsightsJob	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/patient-insights-job/${JobId}	aws:ResourceTag/${TagKey}
Subscription	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/subscription/${SubscriptionId}	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/integration/${IntegrationId}	aws:ResourceTag/${TagKey}
Agent	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/agent/${AgentId}	aws:ResourceTag/${TagKey}
Session	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/session/${SessionId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Connect Health

Amazon Connect Health définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les campagnes sortantes Amazon Connect

Amazon Connect Outbound Campaigns (préfixe de service :`connect-campaigns`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les campagnes sortantes Amazon Connect
- Types de ressources définis par les campagnes sortantes Amazon Connect
- Clés de condition pour les campagnes sortantes Amazon Connect

Actions définies par les campagnes sortantes Amazon Connect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCampaign	Accorde l'autorisation de créer une campagne	Écrire	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCampaign	Accorde l'autorisation de supprimer une campagne	Écrire	campaign*		
DeleteCampaignChannelSubtypeConfig	Autorise la suppression de la configuration du sous-type de chaîne d'une campagne	Écrire	campaign*		
DeleteCampaignCommunicationLimits	Accorde l'autorisation de supprimer la configuration des limites de communication d'une campagne	Écrire	campaign*		
DeleteCampaignCommunicationTime	Autorise la suppression de la configuration du temps de communication d'une campagne	Écrire	campaign*		
DeleteConnectInstanceConfig	Accorde l'autorisation de supprimer les informations de configuration pour une instance Amazon Connect	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConnectInstanceIntegration	Accorde l'autorisation de supprimer les informations d'intégration pour une instance Amazon Connect	Écrire			
DeleteInstanceOnboardingJob	Accorde l'autorisation de supprimer la tâche d'intégration pour une instance Amazon Connect	Écrire			
DescribeCampaign	Accorde l'autorisation de décrire une campagne spécifique	Lecture	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignState	Accorde l'autorisation d'obtenir le statut d'une campagne	Lecture	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignStateBatch	Accorde l'autorisation d'obtenir le statut de campagnes	Lecture	campaign*		
				aws:RequestTag/${TagKey}	
GetConnectInstanceConfig	Accorde l'autorisation d'obtenir des informations de configuration pour une instance Amazon Connect	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInstanceCommunicationLimits	Accorde l'autorisation d'obtenir la configuration des limites de communication d'une instance Amazon Connect	Lecture			
GetInstanceOnboardingJobStatus	Accorde l'autorisation d'obtenir le statut de la tâche d'intégration pour une instance Amazon Connect	Lecture			
ListCampaigns	Accorde l'autorisation de fournir un résumé de toutes les campagnes	List		aws:RequestTag/${TagKey}	
ListConnectInstanceIntegrations	Accorde l'autorisation de fournir un résumé de toutes les intégrations avec une instance Amazon Connect	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	campaign		
				aws:ResourceTag/${TagKey}	
PauseCampaign	Accorde l'autorisation d'interrompre une campagne	Écrire	campaign*		
PutConnectInstanceIntegration	Accorde l'autorisation de mettre une configuration d'intégration avec une instance Amazon Connect	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDialRequestBatch	Accorde l'autorisation de créer des demandes de numérotation pour la campagne spécifiée	Écrire	campaign*		
PutInstanceCommunicationLimits	Accorde l'autorisation de configurer les limites de communication d'une instance Amazon Connect	Écrire			
PutOutboundRequestBatch	Accorde l'autorisation de créer des demandes de numérotation pour la campagne spécifiée	Écrire	campaign*		
PutProfileOutboundRequestBatch	Autorise la création de profils (demandes sortantes) pour la campagne spécifiée	Écrire	campaign*		
ResumeCampaign	Accorde l'autorisation de reprendre une campagne	Écrire	campaign*		
StartCampaign	Accorde l'autorisation de démarrer une campagne	Écrire	campaign*		
StartInstanceOnboardingJob	Accorde l'autorisation de démarrer une tâche d'intégration pour une instance Amazon Connect	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopCampaign	Accorde l'autorisation d'arrêter une campagne	Écrire	campaign*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	campaign*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	campaign*		
				aws:TagKeys	
UpdateCampaignChannelSubtypeConfig	Autorise la mise à jour de la configuration des sous-types de chaînes d'une campagne	Écrire	campaign*		
UpdateCampaignCommunicationLimits	Autorise la mise à jour de la configuration des limites de communication d'une campagne	Écrire	campaign*		
UpdateCampaignCommunicationTime	Autorise la mise à jour de la configuration du temps de communication d'une campagne	Écrire	campaign*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCampaignDialerConfig	Accorde l'autorisation de mettre à jour la configuration de numéroteur d'une campagne	Écrire	campaign*		
UpdateCampaignFlowAssociation	Accorde l'autorisation de mettre à jour l'association de flux d'une campagne	Écrire	campaign*		
UpdateCampaignName	Accorde l'autorisation de mettre à jour le nom d'une campagne	Écrire	campaign*		
UpdateCampaignOutboundCallConfig	Accorde l'autorisation de mettre à jour la configuration des appels sortants d'une campagne	Écrire	campaign*		
UpdateCampaignSchedule	Autorise la mise à jour du calendrier d'une campagne	Écrire	campaign*		
UpdateCampaignSource	Autorise la mise à jour de la source d'une campagne	Écrire	campaign*		

Types de ressources définis par les campagnes sortantes Amazon Connect

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
campaign	`arn:${Partition}:connect-campaigns:${Region}:${Account}:campaign/${CampaignId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les campagnes sortantes Amazon Connect

Amazon Connect Outbound Campaigns définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des actions basées sur la présence de paires clé-valeur de balise dans la requête	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des actions basées sur les paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des actions basées sur la présence de clés d'identification dans la requête	ArrayOfString

Actions, ressources et clés de condition pour Amazon Connect Voice ID

Amazon Connect Voice ID (préfixe de service : `voiceid`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Connect Voice ID
- Types de ressources définis par Amazon Connect Voice ID
- Clés de condition pour Amazon Connect Voice ID

Actions définies par Amazon Connect Voice ID

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateFraudster	Octroie l'autorisation d'associer un fraudeur à une liste de surveillance	Écrire	domain*		
CreateDomain	Accorde l'autorisation de créer un domaine	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWatchlist	Octroie l'autorisation de créer une liste de surveillance	Écrire	domain*		
DeleteDomain	Accorde l'autorisation de supprimer un domaine	Écrire	domain*		
DeleteFraudster	Accorde l'autorisation de supprimer un fraudeur	Écrire	domain*		
DeleteSpeaker	Accorde l'autorisation de supprimer un interlocuteur	Écrire	domain*		
DeleteWatchlist	Octroie l'autorisation de supprimer une liste de surveillance	Écrire	domain*		
DescribeComplianceConsent [autorisation uniquement]	Accorde l'autorisation de décrire un accord sur la conformité	Lecture			
DescribeDomain	Accorde l'autorisation de décrire un domaine	Lecture	domain*		
DescribeFraudster	Accorde l'autorisation de décrire un fraudeur	Lecture	domain*		
DescribeFraudsterRegistrationJob	Accorde l'autorisation de décrire la tâche d'enregistrement d'un fraudeur	Lecture	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSpeaker	Accorde l'autorisation de décrire un interlocuteur	Lecture	domain*		
DescribeSpeakerEnrollmentJob	Accorde l'autorisation de décrire la tâche d'inscription d'un interlocuteur	Lecture	domain*		
DescribeWatchlist	Octroie l'autorisation de décrire une liste de surveillance	Lecture	domain*		
DisassociateFraudster	Octroie l'autorisation de dissocier un fraudeur d'une liste de surveillance	Écrire	domain*		
EvaluateSession	Accorde l'autorisation d'évaluer une session	Écrire	domain*		
ListDomains	Accorde l'autorisation de répertorier les domaines d'un compte	List			
ListFraudsterRegistrationJobs	Accorde l'autorisation de répertorier les tâches d'enregistrement d'un fraudeur pour un domaine	List	domain*		
ListFraudsters	Octroie l'autorisation de répertorier les fraudeurs pour un domaine ou une liste de surveillance	List	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSpeakerEnrollmentJobs	Accorde l'autorisation de répertorier les tâches d'inscription d'un interlocuteur pour un domaine	List	domain*		
ListSpeakers	Accorde l'autorisation de répertorier les interlocuteurs d'un domaine	List	domain*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource Voice ID	Lecture	domain		
ListWatchlists	Octroie l'autorisation de répertorier les listes de surveillance d'un domaine	List	domain*		
OptOutSpeaker	Accorde l'autorisation de désinscrire un interlocuteur	Écrire	domain*		
RegisterComplianceConsent [autorisation uniquement]	Accorde l'autorisation d'enregistrer l'accord sur la conformité	Écrire			
StartFraudsterRegistrationJob	Accorde l'autorisation de démarrer la tâche d'enregistrement d'un fraudeur	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartSpeakerEnrollmentJob	Accorde l'autorisation de démarrer la tâche d'inscription d'un interlocuteur	Écrire	domain*		
TagResource	Accorde l'autorisation d'identifier une ressource Voice ID	Identification	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource Voice ID	Identification	domain		
				aws:TagKeys	
UpdateDomain	Accorde l'autorisation de mettre à jour un domaine	Écrire	domain*		
UpdateWatchlist	Octroie l'autorisation de mettre à jour une liste de surveillance	Écrire	domain*		

Types de ressources définis par Amazon Connect Voice ID

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:voiceid:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Connect Voice ID

Amazon Connect Voice ID définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Connector Service

AWS Connector Service (préfixe de service :`awsconnector`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Connector Service
- Types de ressources définis par AWS Connector Service
- Clés de condition pour AWS Connector Service

Actions définies par AWS Connector Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConnectorHealth [autorisation uniquement]	Récupère toutes les métriques d'état publiées à partir du Server Migration Connector.	Lecture			
RegisterConnector [autorisation uniquement]	Enregistre le AWS AWS connecteur avec le service Connector.	Écrire			
ValidateConnectorId [autorisation uniquement]	Valide l'identifiant du connecteur de migration de serveur enregistré auprès AWS du service Connector.	Lecture			

Types de ressources définis par AWS Connector Service

AWS Connector Service ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Connector Service, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Connector Service

Connector Service ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour l'application AWS Management Console mobile

AWS Management Console L'application mobile (préfixe de service :`consoleapp`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'application AWS Management Console mobile
- Types de ressources définis par l'application AWS Management Console mobile
- Clés de condition pour application AWS Management Console mobile

Actions définies par l'application AWS Management Console mobile

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDeviceIdentity	Octroie l'autorisation de récupérer l'identité d'un appareil d'Application mobile de la console.	Lecture	DeviceIdentity*		
ListDeviceIdentities	Octroie l'autorisation de récupérer une liste des identités d'appareils.	List			

Types de ressources définis par l'application AWS Management Console mobile

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
DeviceIdentity	`arn:${Partition}:consoleapp::${Account}:device/${DeviceId}/identity/${IdentityId}`	

Clés de condition pour application AWS Management Console mobile

L'application mobile de la console ne dispose pas de clés de contexte spécifiques aux services pouvant être utilisées dans l'élément `Condition` des déclarations de politique. Pour obtenir la

liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour la facturation AWS consolidée

AWS La facturation consolidée (préfixe de service :`consolidatedbilling`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par la facturation AWS consolidée
- Types de ressources définis par la facturation AWS consolidée
- Clés de condition pour la facturation AWS consolidée

Actions définies par la facturation AWS consolidée

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut

un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountBillingRole	Accorde l'autorisation d'obtenir le rôle du compte (payeur, lié, régulier)	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
ListLinkedAccounts [autorisation uniquement]	Accorde l'autorisation d'obtenir la liste des member/linked comptes	List			

Types de ressources définis par la facturation AWS consolidée

AWS La facturation consolidée ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Consolidated Billing, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour la facturation AWS consolidée

Consolidated Billing ne dispose pas de clés de contexte spécifiques aux services pouvant être utilisées dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Control Catalog

AWS Control Catalog (préfixe de service :`controlcatalog`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Control Catalog
- Types de ressources définis par AWS Control Catalog
- Clés de condition pour AWS Control Catalog

Actions définies par AWS Control Catalog

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetControl	Autorise le renvoi des informations relatives à un contrôle spécifique	Lecture	control*		
ListCommonControls	Accorde l'autorisation de renvoyer une liste paginée de contrôles courants à partir du catalogue AWS de contrôles	List			
ListControlMappings	Accorde l'autorisation de renvoyer une liste paginée de mappages de contrôles à partir du AWS catalogue de contrôles	List			
ListControls	Accorde l'autorisation de renvoyer une liste paginée de tous les contrôles disponibl	List	control*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	es dans la bibliothèque AWS Control Catalog				
ListDomains	Accorde l'autorisation de renvoyer une liste paginée de domaines à partir du catalogue de AWS contrôle	List			
ListObjectives	Accorde l'autorisation de renvoyer une liste paginée d'objectifs à partir du catalogue de AWS contrôle	List			

Types de ressources définis par AWS Control Catalog

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
common-control	`arn:${Partition}:controlcatalog:::common-control/${CommonControlId}`	
control	`arn:${Partition}:controlcatalog:::control/${ControlId}`	

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:controlcatalog:::domain/${DomainId}`	
objective	`arn:${Partition}:controlcatalog:::objective/${ObjectiveId}`	

Clés de condition pour AWS Control Catalog

Control Catalog ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Control Tower

AWS Control Tower (préfixe de service :`controltower`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Control Tower
- Types de ressources définis par AWS Control Tower
- Clés de condition pour AWS Control Tower

Actions définies par AWS Control Tower

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLandingZone	Octroie l'autorisation de créer une zone de destination.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
CreateManagedAccount [autorisation uniquement]	Autorise la création d'un compte géré par AWS Control Tower	Écrire			
DeleteLandingZone	Autorise la suppression de la zone d'atterrissage de AWS Control Tower	Écrire	LandingZone*		
DeregisterManagedAccount [autorisation uniquement]	Autorise Control Tower à annuler l'enregistrement d'un compte créé via Account Factory AWS	Écrire			
DeregisterOrganizationalUnit [autorisation uniquement]	Accorde l'autorisation de désenregistrer une unité organisationnelle auprès de la direction de AWS Control Tower	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAccountFactoryConfig [autorisation uniquement]	Accorde l'autorisation de décrire la configuration actuelle d'Account Factory	Lecture			
DescribeCoreService [autorisation uniquement]	Permet de décrire les ressources gérées par les comptes principaux dans AWS Control Tower	Lecture			
DescribeGuardrail [autorisation uniquement]	Accorde l'autorisation de décrire une barrière de protection	Lecture			
DescribeGuardrailForTarget [autorisation uniquement]	Accorde l'autorisation de décrire une barrière de protection pour une unité organisationnelle	Lecture			
DescribeLandingZoneConfiguration [autorisation uniquement]	Octroie l'autorisation de décrire la configuration actuelle de la zone de destination	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeManagedAccount [autorisation uniquement]	Accorde l'autorisation de décrire un compte créé via Account Factory	Lecture			
DescribeManagedOrganizationalUnit [autorisation uniquement]	Accorde l'autorisation de décrire une unité organisationnelle d'une AWS organisation gérée par AWS Control Tower	Lecture			
DescribeRegisterOrganizationalUnitOperation [autorisation uniquement]	Octroie l'autorisation de décrire une opération d'enregistrement d'unité d'organisation	Lecture			
DescribeSingleSignOn [autorisation uniquement]	Accorde l'autorisation de décrire la configuration actuelle du AWS Control Tower IAM Identity Center	Lecture			
DisableBaseline	Accorde l'autorisation de désactiver une ligne de base sur une cible	Écrire	EnabledBaseline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableControl	Accorde l'autorisation de supprimer un contrôle d'une unité organisationnelle	Écrire	EnabledControl*		
DisableGuardrail [autorisation uniquement]	Accorde l'autorisation de désactiver la barrière de protection à partir d'une unité organisationnelle	Écrire			
EnableBaseline	Accorde l'autorisation d'activer une ligne de base sur une cible	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
EnableControl	Accorde l'autorisation d'activer un contrôle d'une unité organisationnelle	Écrire	EnabledControl		controltower:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableGuardrail [autorisation uniquement]	Accorde l'autorisation d'activer une barrière de protection dans une unité organisationnelle	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountInfo [autorisation uniquement]	Octroie l'autorisation de décrire une adresse e-mail de compte et de confirmer son existence	Lecture			
GetAvailableUpdates [autorisation uniquement]	Autorise à répertorier les mises à jour disponibles pour le déploiement actuel AWS de Control Tower	Lecture			
GetBaseline	Accorde l'autorisation d'obtenir les détails de référence	Lecture	Baseline*		
GetBaselineOperation	Octroie l'autorisation d'obtenir le statut actuel d'une opération de base donnée	Lecture			
GetControlOperation	Accorde l'autorisation d'obtenir le statut actuel d'un particulier EnabledControl ou d'une DisableControl opération	Lecture			
GetEnabledBaseline	Accorde l'autorisation d'obtenir une base de référence activée	Lecture	EnabledBaseline*		
GetEnabledControl	Accorde l'autorisation d'obtenir un contrôle activé d'une unité organisationnelle.	Lecture	EnabledControl*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGuardrailComplianceStatus [autorisation uniquement]	Accorde l'autorisation d'obtenir l'état actuel de conformité d'une barrière de protection	Lecture			
GetHomeRegion [autorisation uniquement]	Autorise l'accès à la région d'origine de la configuration de la AWS Control Tower	Lecture			
GetLandingZone	Accorde l'autorisation d'obtenir l'état actuel de la configuration de la zone de destination	Lecture	LandingZone*		
GetLandingZoneDriftStatus	Octroie l'autorisation d'obtenir le statut de l'écart de la zone de destination actuelle	Lecture			
GetLandingZoneOperation	Octroie l'autorisation d'obtenir le statut actuel d'une opération de zone de destination particulière.	Lecture			
GetLandingZoneStatus [autorisation uniquement]	Accorde l'autorisation d'obtenir l'état actuel de la configuration de la zone de destination	Lecture			
ListBaselines	Accorde l'autorisation de répertorier les lignes de base	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListControlOperations	Permet de répertorier toutes les opérations de contrôle	List			
ListDirectoryGroups [autorisation uniquement]	Accorde l'autorisation de répertorier les groupes de répertoires actuellement disponibles via IAM Identity Center	List			
ListDriftDetails	Permet de répertorier les occurrences de dérive dans AWS Control Tower	Lecture			
ListEnabledBaselines	Accorde l'autorisation de répertorier les lignes de base activées	List			
ListEnabledControls	Accorde l'autorisation de répertorier tous les contrôles activés dans une unité organisationnelle spécifiée	List			
ListEnabledGuardrails [autorisation uniquement]	Accorde l'autorisation de répertorier les barrières de protection actuellement activées	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListExtendGovernancePrecheckDetails [autorisation uniquement]	Octroie l'autorisation de répertorier les informations de vérification préalable d'une unité d'organisation	List			
ListExternalConfigRuleCompliance	Accorde l'autorisation de répertorier la conformité des règles de AWS configuration externes	Lecture			
ListGuardrailViolations [autorisation uniquement]	Accorde l'autorisation de répertorier les violations existantes des barrières de protection	List			
ListGuardrails [autorisation uniquement]	Accorde l'autorisation de répertorier toutes les barrières de protection disponibles	List			
ListGuardrailsForTarget [autorisation uniquement]	Accorde l'autorisation de répertorier les barrières de protection et leur état actuel pour une unité organisationnelle	List			
ListLandingZoneOperations	Permet de répertorier toutes les opérations de zone d'atterrissage	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLandingZones	Octroie l'autorisation de répertorier toutes les zones de destination.	List			
ListManagedAccounts [autorisation uniquement]	Permet de répertorier les comptes gérés via AWS Control Tower	List			
ListManagedAccountsForGuardrail [autorisation uniquement]	Accorde l'autorisation de répertorier les comptes gérés avec une barrière de protection spécifique appliquée	List			
ListManagedAccountsForParent [autorisation uniquement]	Accorde l'autorisation de répertorier les comptes gérés sous une unité organisationnelle	List			
ListManagedOrganizationalUnits [autorisation uniquement]	Permet de répertorier les unités organisationnelles gérées par AWS Control Tower	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListManagedOrganizationalUnitsForGuardrail [autorisation uniquement]	Accorde l'autorisation de répertorier les unités organisationnelles gérées auxquelles une barrière de protection spécifiée a été appliquée	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	EnabledBaseline		
			EnabledControl		
			LandingZone		
ManageOrganizationalUnit [autorisation uniquement]	Accorde l'autorisation de configurer une unité organisationnelle qui sera gérée par AWS Control Tower	Écrire			
PerformPreLaunchChecks [autorisation uniquement]	Octroie l'autorisation d'effectuer des validations dans un compte	Lecture			
ResetEnabledBaseline	Accorde l'autorisation de réinitialiser une ligne de base activée	Écrire	EnabledBaseline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResetEnabledControl	Accorde l'autorisation de réinitialiser un contrôle activé pour une unité organisationnelle	Écrire	EnabledControl*		
ResetLandingZone	Octroie l'autorisation de réinitialiser une zone de destination.	Écrire	LandingZone*		
SetupLandingZone [autorisation uniquement]	Autorise la création ou la mise à jour de la zone d'atterrissage AWS de la Control Tower	Écrire			
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	EnabledBaseline		
			EnabledControl		
			LandingZone		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	EnabledBaseline		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			EnabledControl		
			LandingZone		
				aws:TagKeys	
UpdateAccountFactoryConfig [autorisation uniquement]	Accorde l'autorisation de mettre à jour la configuration d'Account Factory	Écrire			
UpdateEnabledBaseline	Accorde l'autorisation de mettre à jour une ligne de base activée	Écrire	EnabledBaseline*		
UpdateEnabledControl	Octroie l'autorisation de mettre à jour un contrôle activé pour une unité organisationnelle.	Écrire	EnabledControl*		
UpdateLandingZone	Octroie l'autorisation de mettre à jour une zone de destination.	Écrire	LandingZone*		

Types de ressources définis par AWS Control Tower

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
EnabledControl	`arn:${Partition}:controltower:${Region}:${Account}:enabledcontrol/${EnabledControlId}`	aws:ResourceTag/${TagKey}
Baseline	`arn:${Partition}:controltower:${Region}::baseline/${BaselineId}`	
EnabledBaseline	`arn:${Partition}:controltower:${Region}:${Account}:enabledbaseline/${EnabledBaselineId}`	aws:ResourceTag/${TagKey}
LandingZone	`arn:${Partition}:controltower:${Region}:${Account}:landingzone/${LandingZoneId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Control Tower

AWS Control Tower définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le rapport sur les AWS coûts et l'utilisation

AWS Le rapport sur les coûts et l'utilisation (préfixe de service :`cur`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le rapport sur les AWS coûts et l'utilisation
- Types de ressources définis par le rapport sur les AWS coûts et l'utilisation
- Clés de condition pour le rapport sur les AWS coûts et l'utilisation

Actions définies par le rapport sur les AWS coûts et l'utilisation

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteReportDefinition	Accorde l'autorisation d'effacer la définition du rapport d'utilisation et de coût	Écrire	cur*		
DescribeReportDefinitions	Accorde l'autorisation d'obtenir les définitions du rapport d'utilisation et de coût	Lecture			
GetClassicReport [autorisation uniquement]	Accorde l'autorisation d'obtenir le rapport CSV de facturation	Lecture			
GetClassicReportPreferences [autorisation uniquement]	Accorde l'autorisation d'obtenir le statut d'habilitation de rapport classique pour les rapports d'utilisation	Lecture			
GetUsageReport [autorisation uniquement]	Accorde l'autorisation d'obtenir la liste des AWS services, le type d'utilisation et le fonctionnement pour le flux de travail du rapport d'utilisation. Autorise ou refuse également le téléchargement des rapports d'utilisation	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture	cur*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ModifyReportDefinition	Accorde l'autorisation de modifier la définition du rapport d'utilisation et de coût	Écrire	cur*		
PutClassicReportPreferences [autorisation uniquement]	Accorde l'autorisation d'activer des rapports classiques	Écrire			
PutReportDefinition	Accorde l'autorisation de rédiger une définition du rapport d'utilisation et de coût	Écrire	cur*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	cur*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	cur*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
ValidateReportDestination [autorisation uniquement]	Accorde l'autorisation de valider si le compartiment S3 existe avec les autorisations appropriées pour la livraison du CUR	Lecture			

Types de ressources définis par le rapport sur les AWS coûts et l'utilisation

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cur	`arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}`	

Clés de condition pour le rapport sur les AWS coûts et l'utilisation

AWS Le rapport sur les coûts et l'utilisation définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le service AWS Cost Explorer

AWS Le service Cost Explorer (préfixe de service :`ce`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service AWS Cost Explorer
- Types de ressources définis par AWS Cost Explorer Service
- Clés de condition pour AWS le service Cost Explorer

Actions définies par le service AWS Cost Explorer

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAnomalyMonitor	Accorde l'autorisation de créer un moniteur d'anomalies	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	Accorde l'autorisation de créer un abonnement aux anomalies	Écriture		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateCostCategoryDefinition	Accorde l'autorisation de créer une catégorie de coûts avec le nom et les règles demandés.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationSubscription [autorisation uniquement]	Accorde l'autorisation de créer des alertes d'expiration de réservation.	Écriture			
CreateReport [autorisation uniquement]	Accorde l'autorisation de créer des rapports Cost Explorer.	Écriture			
DeleteAnomalyMonitor	Accorde l'autorisation de supprimer un moniteur d'anomalies	Écriture	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	Accorde l'autorisation de supprimer un abonnement aux anomalies	Écriture	anomalysubscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Accorde l'autorisation de supprimer une catégorie de coûts	Écriture	costcategory*		
				aws:ResourceTag/${TagKey}	
DeleteNotificationSubscription [autorisation uniquement]	Accorde l'autorisation de supprimer les alertes d'expiration de réservation.	Écriture			
DeleteReport [autorisation uniquement]	Accorde l'autorisation de supprimer les rapports Cost Explorer.	Écriture			
DescribeCostCategoryDefinition	Accorde l'autorisation d'extraire des descriptions telles que le nom, l'ARN, les règles, la définition et les dates de validité d'une catégorie de coûts	Lecture	costcategory*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeNotificationSubscription [autorisation uniquement]	Accorde l'autorisation d'afficher les alertes d'expiration de réservation.	Lecture			
DescribeReport [autorisation uniquement]	Accorde l'autorisation d'afficher la page des rapports Cost Explorer.	Lecture			
GetAnomalies	Accorde l'autorisation d'extraire les anomalies	Lecture	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	Accorde l'autorisation d'interroger les moniteurs d'anomalies	Lecture	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	Accorde l'autorisation d'interroger les abonnements aux anomalies	Lecture	anomalysubscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetApproximateUsageRecords	Autorise à récupérer le nombre approximatif d'enregistrements d'utilisation pour la ressource, le niveau et les préférences de granularité horaire choisis, dérivés de l'utilisation du mois dernier	Lecture			
GetCommitmentPurchaseAnalysis	Accorde l'autorisation de récupérer l'analyse des achats engagés pour votre compte	Lecture			
GetConsoleActionSetEnforced [autorisation uniquement]	Octroie l'autorisation de voir si des actions IAM existantes ou détaillées sont utilisées pour contrôler l'autorisation des consoles de facturation, de gestion des coûts et de compte	Lecture			
GetCostAndUsage	Accorde l'autorisation de récupérer les métriques de coût et d'utilisation pour votre compte	Lecture	billingview		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCostAndUsageComparisons	Accorde l'autorisation de récupérer les comparaisons de coûts et d'utilisation pour votre compte	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
GetCostAndUsageWithResources	Accorde l'autorisation de récupérer les métriques de coût et d'utilisation avec des ressources pour votre compte	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
GetCostCategories	Accorde l'autorisation d'interroger les noms et les valeurs des catégories de coûts pour une durée déterminée	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
GetCostComparisonDrivers	Autorise à récupérer les inducteurs de coûts de votre compte	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
GetCostForecast	Accorde l'autorisation de récupérer une prévision des coûts pour une période de prévision	Lecture	billingview		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetDimensionValues	Accorde l'autorisation de récupérer toutes les valeurs de filtre disponibles pour un filtre pour une période donnée	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
GetPreferences [autorisation uniquement]	Accorde l'autorisation d'afficher la page des préférences Cost Explorer.	Lecture			
GetReservationCoverage	Accorde l'autorisation de récupérer la couverture de réservation pour votre compte	Lecture			
GetReservationPurchaseRecommendation	Accorde l'autorisation de récupérer les recommandations de réservation pour votre compte	Lecture			
GetReservationUtilization	Accorde l'autorisation de récupérer l'utilisation de réservation pour votre compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRightsizingRecommendation	Accorde l'autorisation de récupérer les recommandations de dimensionnement correct pour votre compte	Lecture			
GetSavingsPlanPurchaseRecommendationDetails	Octroie l'autorisation de récupérer les recommandations Savings Plans de votre compte.	Lecture			
GetSavingsPlansCoverage	Accorde l'autorisation de récupérer la couverture Savings Plans pour votre compte	Lecture			
GetSavingsPlansPurchaseRecommendation	Accorde l'autorisation de récupérer les recommandations Savings Plans pour votre compte	Lecture			
GetSavingsPlansUtilization	Accorde l'autorisation de récupérer l'utilisation de Savings Plans pour votre compte	Lecture			
GetSavingsPlansUtilizationDetails	Accorde l'autorisation de récupérer les détails d'utilisation de Savings Plans pour votre compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTags	Accorde l'autorisation d'interroger les balises pour une durée déterminée	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
GetUsageForecast	Accorde l'autorisation de récupérer une prévision d'utilisation pour une période de prévision	Lecture	billingview		
				aws:ResourceTag/${TagKey}	
ListCommitmentPurchaseAnalyses	Accorde l'autorisation de récupérer une liste de l'historique de vos analyses d'achats et d'engagements	List			
ListCostAllocationTagBackfillHistory	Autorise à répertorier l'historique de remplissage des balises de répartition des coûts	List			
ListCostAllocationTags	Accorde l'autorisation de répertorier les identifications d'une allocation des coûts	List			
ListCostCategoryDefinitions	Accorde l'autorisation pour récupérer les noms, l'ARN et les dates de validité de toutes les Cost Categories	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCostCategoryResourceAssociations	Accorde l'autorisation de récupérer les associations de ressources de toutes les Cost Categories définies dans le compte	List			
ListSavingsPlansPurchaseRecommendationGeneration	Accorde l'autorisation de récupérer une liste de vos générations de recommandations historiques	List			
ListTagsForResource	Accorde l'autorisation de répertorier des identifications pour une ressource Cost Explorer	Lecture	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	Accorde l'autorisation de fournir des commentaires sur les anomalies détectées	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartCommitmentPurchaseAnalysis	Accorde l'autorisation de demander une analyse des achats liés aux engagements	Écrire			
StartCostAllocationTagBackfill	Accorde l'autorisation de demander un remblayage par étiquette de répartition des coûts	Écrire			
StartSavingsPlansPurchaseRecommendationGeneration	Accorde l'autorisation de demander la génération d'une recommandation de Savings Plans	Écrire			
TagResource	Accorde l'autorisation d'étiqueter une ressource Cost Explorer	Identification	anomalymonitor		
			anomalysubscription		
			costcategory		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les identifications d'une ressource Cost Explorer	Identification	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	Accorde l'autorisation de mettre à jour un moniteur d'anomalies existant	Écriture	anomalymonitor*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAnomalySubscription	Accorde l'autorisation de mettre à jour un abonnement aux anomalies existant	Écrire	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [autorisation uniquement]	Octroie l'autorisation de modifier l'utilisation ou non des actions IAM existantes ou détaillées pour contrôler l'autorisation des consoles de facturation, de gestion des coûts et de compte	Écrire			
UpdateCostAllocationTagsStatus	Accorde l'autorisation de mettre à jour le statut existant des identifications d'une allocation de coûts	Écrire			
UpdateCostCategoryDefinition	Accorde l'autorisation de mettre à jour une catégorie de coûts existante	Écriture	costcategory*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNotification Subscription [autorisation uniquement]	Accorde l'autorisation de mettre à jour les alertes d'expiration de réservation.	Écriture			
UpdatePreferences [autorisation uniquement]	Accorde l'autorisation de modifier la page des préférences Cost Explorer.	Écriture			
UpdateReport [autorisation uniquement]	Accorde l'autorisation de mettre à jour les rapports Cost Explorer.	Écrire			

Types de ressources définis par AWS Cost Explorer Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
anomalysubscription	`arn:${Partition}:ce::${Account}:anomalysubscription/${Identifier}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
anomalymonitor	`arn:${Partition}:ce::${Account}:anomalymonitor/${Identifier}`	aws:ResourceTag/${TagKey}
costcategory	`arn:${Partition}:ce::${Account}:costcategory/${Identifier}`	aws:ResourceTag/${TagKey}
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS le service Cost Explorer

AWS Le service Cost Explorer définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le hub d'optimisation des AWS coûts

AWS Le hub d'optimisation des coûts (préfixe de service :`cost-optimization-hub`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS Cost Optimization Hub
- Types de ressources définis par le AWS Cost Optimization Hub
- Clés de condition pour le hub d'optimisation des AWS coûts

Actions définies par le AWS Cost Optimization Hub

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPreferences	Octroie l'autorisation d'obtenir les préférences.	Lecture			
GetRecommendation	Octroie l'autorisation d'obtenir la configuration des ressource	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	s et l'impact financier estimé d'une recommandation.				
ListEfficiencyMetrics	Permet de répertorier les scores des indicateurs d'efficacité par groupe	List			
ListEnrollmentStatuses	Octroie l'autorisation de répertorier les statuts d'inscription pour le compte spécifié ou pour tous les membres d'un compte de gestion.	List			
ListRecommendationSummaries	Octroie l'autorisation de répertorier les récapitulatifs des recommandations par groupe.	List			cost-optimization-hub:GetRecommendation
ListRecommendations	Octroie l'autorisation de répertorier les vues des récapitulatifs des recommandations.	List			cost-optimization-hub:GetRecommendation
UpdateEnrollmentStatus	Accorde l'autorisation de mettre à jour le statut d'inscription	Écrire			
UpdatePreferences	Octroie l'autorisation de mettre à jour les préférences.	Écrire			

Types de ressources définis par le AWS Cost Optimization Hub

AWS Cost Optimization Hub ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au hub d'optimisation des coûts AWS , spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le hub d'optimisation des AWS coûts

Le hub d'optimisation des coûts ne comporte aucune clé de contexte propre au service pouvant être utilisée dans l'élément `Condition` des instructions de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le service de vérification AWS client

AWS Le service de vérification client (préfixe de service :`customer-verification`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service de vérification des AWS clients
- Types de ressources définis par le service de vérification AWS client
- Clés de condition pour AWS le service de vérification client

Actions définies par le service de vérification des AWS clients

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCustomerVerificationDetails [autorisation uniquement]	Accorde l'autorisation de créer des données de vérification des clients	Écrire			
CreateUploadUrls [autorisation uniquement]	Accorde l'autorisation de créer un téléchargement URLs	Écrire			
GetCustomerVerificationDetails [autorisation uniquement]	Accorde l'autorisation d'obtenir les données de vérification des clients	Lecture			
GetCustomerVerificationEligibility [autorisation uniquement]	Accorde l'autorisation d'obtenir l'éligibilité de la vérification des clients	Lecture			
UpdateCustomerVerificationDetails [autorisation uniquement]	Accorde l'autorisation de mettre à jour les données de vérification des clients	Écrire			

Types de ressources définis par le service de vérification AWS client

AWS Le service de vérification client ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au service de vérification des clients AWS , spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS le service de vérification client

Le service de vérification des clients ne dispose pas de clés de contexte spécifiques aux services qui peuvent être utilisées dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Data Exchange

AWS Data Exchange (préfixe de service :`dataexchange`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Data Exchange
- Types de ressources définis par AWS Data Exchange
- Clés de condition pour AWS Data Exchange

Actions définies par AWS Data Exchange

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptDataGrant	Accorde l'autorisation d'accepter une autorisation de transfert de données	Écrire	data-grants*		
CancelJob	Accorde l'autorisation d'annuler une tâche	Écrire	jobs*		
CreateAsset [autorisation uniquement]	Accorde l'autorisation de créer une ressource (par exemple, dans une tâche)	Écrire	revisions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataGrant	Accorde l'autorisation de créer une autorisation de données	Écrire	data-grants*		dataexchange:PublishToDataGrant
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Accorde l'autorisation de créer un ensemble de données	Écrire	data-sets*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventAction	Accorde l'autorisation de créer une action d'événement	Écrire	event-actions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Accorde l'autorisation de créer une tâche pour importer ou exporter des ressources	Écrire	jobs*		
				dataexchange:JobType	
CreateRevision	Accorde l'autorisation de créer une révision	Écrire	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAsset	Accorde l'autorisation de supprimer une ressource	Écrire	assets*		
DeleteDataGrant	Accorde l'autorisation de supprimer une autorisation de données	Écrire	data-grants*		
DeleteDataSet	Accorde l'autorisation de supprimer un ensemble de données	Écrire	data-sets*		
			entitled-data-sets*		
DeleteEventAction	Accorde l'autorisation de supprimer une action d'événement	Écrire	event-actions*		
DeleteRevision	Accorde l'autorisation de supprimer une révision	Écrire	revisions*		
GetAsset	Accorde l'autorisation d'obtenir des informations sur une ressource et de les exporter (par exemple, dans une tâche)	Lecture	assets*		
			entitled-assets*		
GetDataGrant	Accorde l'autorisation d'obtenir une subvention de données	Lecture	data-grants*		
GetDataSet	Accorde l'autorisation d'obtenir des informations sur un ensemble de données	Lecture	data-sets*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			entitled-data-sets*		
GetEventAction	Accorde l'autorisation d'obtenir une action d'événement	Lecture	event-actions*		
GetJob	Accorde l'autorisation d'obtenir des informations sur une tâche	Lecture	jobs*		
GetReceivedDataGrant	Accorde l'autorisation d'obtenir une subvention pour les données reçues	Lecture	data-grants*		
GetRevision	Accorde l'autorisation d'obtenir des informations sur une révision	Lecture	entitled-revisions*		
			revisions*		
ListDataGrants	Accorde l'autorisation de répertorier les autorisations de données pour le compte	List			
ListDataSetRevisions	Accorde l'autorisation de répertorier les révisions d'un ensemble de données	List	data-sets*		
			entitled-data-sets*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDataSets	Accorde l'autorisation de répertorier les ensembles de données du compte	List			
ListEventActions	Accorde l'autorisation de répertorier les actions d'événements pour le compte	List			
ListJobs	Accorde l'autorisation de répertorier les tâches du compte	List			
ListReceivedDataGrants	Accorde l'autorisation de répertorier les données reçues, accorde des autorisations pour le compte	List			
ListRevisionAssets	Accorde l'autorisation d'obtenir la liste des ressources d'une révision	List	entitled-revisions *		
			revisions *		
ListTagsForResource	Accorde l'autorisation de répertorier les balises que vous avez associées à la ressource spécifiée	List	assets		
			data-grants		
			data-sets		
			event-actions		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			revisions		
PublishDataSet [autorisation uniquement]	Accorde l'autorisation de publier un ensemble de données sur un produit	Écrire	data-sets*		
PublishToDataGrant [autorisation uniquement]	Accorde l'autorisation de publier un ensemble de données dans le cadre d'une subvention de données	Écrire	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RevokeRevision	Accorde l'autorisation de revoquer l'accès d'un abonné à une révision	Écrire	revisions*		
SendApiAsset	Accorde l'autorisation d'envoyer une requête à un actif d'API	Écrire	assets*		
			entitled-assets*		
SendDataSetNotification	Accorde l'autorisation d'envoyer une notification aux abonnés d'un ensemble de données	Écrire	data-sets*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartJob	Accorde l'autorisation de démarrer une tâche	Écrire	jobs*		dataexchange:CreateAsset dataexchange:DeleteDataSet dataexchange:GetAsset dataexchange:GetDataSet dataexchange:GetRevision dataexchange:PublishDataSet redshift:AuthorizeDataShare
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à la ressource spécifiée	Balisage	assets		
			data-grants		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			data-sets		
			event-actions		
			revisions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises de la ressource spécifiée	Identification	assets		
			data-grants		
			data-sets		
			event-actions		
			revisions		
				aws:TagKeys	
UpdateAsset	Accorde l'autorisation d'obtenir les informations de mise à jour d'une ressource	Écrire	assets*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataSet	Accorde l'autorisation de mettre à jour les informations relatives à un ensemble de données	Écrire	data-sets*		
UpdateEventAction	Accorde l'autorisation de mettre à jour les informations d'une action d'événement	Écrire	event-actions*		
UpdateRevision	Accorde l'autorisation de mettre à jour les informations relatives à une révision	Écrire	revisions*		dataexchange:PublishDataSet dataexchange:PublishToDataGrant

Types de ressources définis par AWS Data Exchange

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
jobs	arn:${Partition}:dataexchange:${Region}:${Account}:jobs/${JobId}	dataexchange:JobType
data-sets	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}	aws:ResourceTag/${TagKey}
entitled-data-sets	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}	
revisions	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}	aws:ResourceTag/${TagKey}
entitled-revisions	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}	
assets	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	aws:ResourceTag/${TagKey}
entitled-assets	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	
event-actions	arn:${Partition}:dataexchange:${Region}:${Account}:event-actions/${EventActionId}	aws:ResourceTag/${TagKey}
data-grants	arn:${Partition}:dataexchange:${Region}:${Account}:data-grants/${DataGrantId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Data Exchange

AWS Data Exchange définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisé pour chacune des balises obligatoires dans la demande de création	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur de balise associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de balises obligatoires dans la demande de création	ArrayOfString
dataexchange:JobType	Filtre l'accès en fonction du type de tâche spécifié	String

Actions, ressources et clés de condition pour Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager (préfixe de service : `dlm`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Data Lifecycle Manager
- Types de ressources définis par Amazon Data Lifecycle Manager
- Clés de condition pour Amazon Data Lifecycle Manager

Actions définies par Amazon Data Lifecycle Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLifecyclePolicy	Accorde l'autorisation de créer une politique de cycle de vie des données pour gérer la création et la conservation planifiées des instantanés Amazon EBS. Vous pouvez avoir 100 politiques maximum	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLifecyclePolicy	Accorde l'autorisation de supprimer une politique de cycle de vie des données existante. En outre, cette action interrompt la création et la suppression d'instantanés spécifiés par la politique. Les instantanés existants ne sont pas affectés	Écrire	policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLifecyclePolicies	Accorde l'autorisation de renvoyer une liste de descriptions récapitulatives des politiques de cycle de vie des données	List			
GetLifecyclePolicy	Accorde l'autorisation de renvoyer une description complète d'une seule politique de cycle de vie des données	Lecture	policy*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises associées à une ressource	Lecture	policy*		
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour des balises d'une ressource	Identification	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises associées à une ressource.	Identification	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	Accorde l'autorisation de mettre à jour une politique de cycle de vie des données existante	Écrire	policy*		

Types de ressources définis par Amazon Data Lifecycle Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
policy	`arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Data Pipeline

AWS Data Pipeline (préfixe de service :`datapipeline`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Data Pipeline
- Types de ressources définis par AWS Data Pipeline
- Clés de condition pour AWS Data Pipeline

Actions définies par AWS Data Pipeline

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivatePipeline	Accorde l'autorisation de valider le pipeline spécifié et démarre le traitement des tâches du pipeline. Si le pipeline ne réussit pas la validation, l'activation échoue	Écrire	pipeline*		
				datapipeline:PipelineCreator	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				datapipeline:Tag/${TagKey} datapipeline:workerGroup	
AddTags	Accorde l'autorisation d'ajouter ou de modifier des identifications pour le pipeline spécifié	Identification	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePipeline	Accorde l'autorisation de créer un pipeline vide	Écrire		aws:RequestTag/${TagKey} aws:TagKeys datapipeline:Tag/${TagKey}	datapipeline:AddTags
DeactivatePipeline	Accorde l'autorisation de désactiver le pipeline en cours d'exécution spécifié	Écrire	pipeline*	datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePipeline	Accorde l'autorisation de supprimer un pipeline, sa définition de pipeline et son historique d'exécution	Écrire	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
DescribeObjects	Accorde l'autorisation d'obtenir des définitions d'objet pour un jeu d'objets associé au pipeline	Lecture	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
DescribePipelines	Accorde l'autorisation d'extraire des métadonnées relatives à un ou plusieurs pipelines	Lecture	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EvaluateExpression	Autorise les exécuteurs de tâches à appeler EvaluateExpression, à évaluer une chaîne dans le contexte de l'objet spécifié	Lecture	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
GetAccountLimits [autorisation uniquement]	Accorde l'autorisation d'appeler GetAccountLimits	List			
GetPipelineDefinition	Accorde l'autorisation d'obtenir la définition du pipeline spécifié	Lecture	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPipelines	Accorde l'autorisation de répertorier les identifiants de tous les pipelines actifs auxquels vous avez l'autorisation d'accéder	List			
PollForTask	Autorise les exécuteurs de tâches à appeler PollForTask ou à recevoir une tâche à effectuer depuis AWS Data Pipeline	Écrire		datapipeline:workerGroup	
PutAccountLimits [autorisation uniquement]	Accorde l'autorisation d'appeler PutAccountLimits	Écrire			
PutPipelineDefinition	Accorde l'autorisation d'ajouter des tâches, des planifications et des conditions préalables au pipeline spécifié	Écrire	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
QueryObjects	Accorde l'autorisation d'interroger le pipeline spécifié pour obtenir les noms des objets correspondant à l'ensemble de conditions spécifié	Lecture	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
RemoveTags	Accorde l'autorisation de supprimer des identifications existantes du pipeline spécifié	Identification	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ReportTaskProgress	Autorise les exécuteurs de tâches à appeler ReportTaskProgress, lorsqu'une tâche leur est affectée, pour confirmer qu'elle contient la tâche	Écrire	pipeline*		
ReportTaskRunnerHeartbeat	Autorise les exécutants de tâches à appeler ReportTaskRunnerHeartbeat toutes les 15 minutes pour indiquer qu'ils sont opérationnels	Écrire			
SetStatus	Accorde l'autorisation de demander que le statut des objets de pipeline physiques ou logiques spécifiés soit mis à jour dans le pipeline spécifié	Écrire	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
SetTaskStatus	Autorise les exécuteurs de tâches SetTaskStatus à appeler pour informer AWS Data Pipeline qu'une tâche est terminée et fournir des informations sur le statut final	Écrire	pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ValidatePipelineDefinition	Accorde l'autorisation de valider la définition du pipeline spécifié pour s'assurer qu'il est correctement formé et peut être exécuté sans erreur	Lecture	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Types de ressources définis par AWS Data Pipeline

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
pipeline	`arn:${Partition}:datapipeline:${Region}:${Account}:pipeline/${PipelineId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Data Pipeline

AWS Data Pipeline définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
datapipeline:PipelineCreator	Filtre l'accès par l'utilisateur IAM qui a créé le pipeline	ArrayOfString
datapipeline:Tag/${TagKey}	Filtre l'accès par key/value paire spécifiée par le client qui peut être attachée à une ressource	String
datapipeline:workerGroup	Filtre l'accès par le nom d'un groupe d'employés pour lequel un Task Runner récupère le travail	ArrayOfString

Actions, ressources et clés de condition pour le service AWS de migration de base de données

AWS Database Migration Service (préfixe de service :dms) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS Database Migration Service
- Types de ressources définis par AWS Database Migration Service
- Clés de condition pour le Service AWS de Migration de Base de Données

Actions définies par le AWS Database Migration Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTagsToResource	Accorde l'autorisation d'ajouter de balises de métadonnées aux ressources DMS, y compris les instances de réplication, les points de	Balisage	Certificate		
			DataMigration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	terminaison, les groupes de sécurité et les tâches de migration		DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	Accorde l'autorisation d'appliquer une action de maintenance en attente à une ressource (par exemple, à une instance de réplication)	Écrire	ReplicationInstance*		
AssociateExtensionPack	Accorde l'autorisation d'associer un pack d'extension	Écrire	MigrationProject*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchStartRecommendations	Octroie l'autorisation de démarrer l'analyse d'un maximum de 20 bases de données sources afin de recommander des moteurs cibles pour chaque base de données source	Écrire			
CancelMetadataModelConversion	Accorde l'autorisation d'annuler une seule opération de conversion de modèle de métadonnées démarrée avec StartMetadataModelConversion	Écrire	MigrationProject*		
CancelMetadataModelCreation	Accorde l'autorisation d'annuler une seule opération de création de modèle de métadonnées démarrée avec StartMetadataModelCreation	Écrire	MigrationProject*		
CancelReplicationTaskAssessmentRun	Accorde l'autorisation d'annuler une seule exécution d'évaluation de prémigration	Écrire	ReplicationTaskAssessmentRun*		
CreateDataMigration	Accorde l'autorisation de créer une migration de base de données à l'aide des paramètres fournis.	Écrire	MigrationProject*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateDataProvider	Accorde l'autorisation de créer un fournisseur de données à l'aide des paramètres fournis	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEndpoint	Accorde l'autorisation de créer un point de terminaison à l'aide des paramètres fournis	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateEventSubscription	Accorde l'autorisation de créer un abonnement aux notifications d'événements AWS DMS	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFleetAdvisorCollector	Accorde l'autorisation de créer un collecteur Fleet Advisor à l'aide des paramètres spécifiés	Écrire			iam:PassRole
CreateInstanceProfile	Accorde l'autorisation de créer un profil d'instance à l'aide des paramètres fournis	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateMigrationProject	Accorde l'autorisation de créer un projet de migration à l'aide des paramètres fournis	Écrire	DataProvider* InstanceProfile*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateOutboundIntegration [autorisation uniquement]	Autorise DMS à créer des ressources pour des intégrations sans ETL avec des bases de données autogérées	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReplicationConfig	Accorde l'autorisation de créer une configuration de réplication à l'aide des paramètres fournis.	Écrire	Endpoint*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationInstance	Accorde l'autorisation de créer une instance de réplication à l'aide des paramètres spécifiés	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReplicationSubnetGroup	Accorde l'autorisation de créer un groupe de sous-réseaux de réplication à partir de la liste des sous-réseaux d'un IDs VPC	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationTask	Accorde l'autorisation de créer une tâche de réplication à l'aide des paramètres spécifiés	Écriture	Endpoint* ReplicationInstance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
DeleteCertificate	Accorde l'autorisation de supprimer le certificat spécifié	Écriture	Certificate*		
DeleteConnection	Accorde l'autorisation de supprimer la connexion spécifiée entre une instance de réplication et un point de terminaison.	Écrire	Endpoint* ReplicationInstance*		
DeleteDataMigration	Accorde l'autorisation de supprimer la migration de base de données spécifiée.	Écrire	DataMigration*		
DeleteDataProvider	Accorde l'autorisation de supprimer le fournisseur de données spécifié	Écrire	DataProvider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEndpoint	Accorde l'autorisation de supprimer le point de terminaison spécifié	Écrire	Endpoint*		
DeleteEventSubscription	Autorise la suppression d'un abonnement à un événement AWS DMS	Écrire	EventSubscription*		
DeleteFleetAdvisorCollector	Accorde l'autorisation de supprimer le collecteur Fleet Advisor spécifié	Écrire			
DeleteFleetAdvisorDatabases	Accorde l'autorisation de supprimer les bases de données Fleet Advisor spécifiées	Écrire			
DeleteInstanceProfile	Accorde l'autorisation de supprimer le profil d'instance spécifié	Écrire	InstanceProfile*		
DeleteMigrationProject	Accorde l'autorisation de supprimer le projet de migration spécifié	Écrire	MigrationProject*		
DeleteReplicationConfig	Accorde l'autorisation de supprimer la configuration de réplication spécifiée.	Écrire	ReplicationConfig*		
DeleteReplicationInstance	Accorde l'autorisation de supprimer l'instance de réplication spécifiée	Écriture	ReplicationInstance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteReplicationSubnetGroup	Accorde l'autorisation de supprimer un groupe de sous-réseaux	Écriture	ReplicationSubnetGroup*		
DeleteReplicationTask	Accorde l'autorisation de supprimer la tâche de réplication spécifiée	Écriture	ReplicationTask*		
DeleteReplicationTaskAssessmentRun	Accorde l'autorisation de supprimer l'enregistrement d'une seule exécution d'évaluation de prémigration	Écrire	ReplicationTaskAssessmentRun*		
DescribeAccountAttributes	Accorde l'autorisation de répertorier tous les attributs AWS DMS d'un compte client	Lecture			
DescribeApplicableIndividualAssessments	Accorde l'autorisation de répertorier les évaluations individuelles que vous pouvez spécifier pour une nouvelle exécution d'évaluation de prémigration	Lecture	ReplicationInstance ReplicationTask		
DescribeCertificates	Accorde l'autorisation de fournir une description du certificat	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeConnections	Accorde l'autorisation de décrire le statut des connexions établies entre l'instance de réplication et un point de terminaison	Lecture			
DescribeConversionConfiguration	Accorde l'autorisation de renvoyer des informations sur la configuration du projet de conversion de schéma DMS	Lecture	MigrationProject*		
DescribeDataMigrations	Accorde l'autorisation de renvoyer des informations sur les migrations de base de données de votre compte dans la région spécifiée.	Lecture			
DescribeEndpointSettings	Accord l'autorisation de renvoyer les paramètres de point de terminaison possibles disponibles lorsque vous créez un point de terminaison pour un moteur de base de données spécifique	Lecture			
DescribeEndpointTypes	Accorde l'autorisation de renvoyer des informations sur le type de points de terminaison disponibles	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEndpoints	Accorde l'autorisation de renvoyer des informations sur les points de terminaison de votre compte dans la région actuelle	Lecture			
DescribeEngineVersions	Accorde l'autorisation de renvoyer des informations sur les versions disponibles pour les instances de réplication DMS.	Lecture			
DescribeEventCategories	Accorde l'autorisation de répertorier les catégories de tous les types de sources d'événement ou, si la valeur est spécifiée, d'un type de source donné	Lecture			
DescribeEventSubscriptions	Accorde l'autorisation de répertorier tous les abonnements aux événements d'un compte client	Lecture			
DescribeEvents	Accorde l'autorisation de répertorier les événements pour un identificateur source et un type de source donnés	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFleetAdvisorCollectors	Accorde l'autorisation de renvoyer une liste paginée des collecteurs Fleet Advisor sur votre compte en fonction des paramètres de filtrage	Lecture			
DescribeFleetAdvisorDatabases	Accorde l'autorisation de renvoyer une liste paginée des bases de données Fleet Advisor sur votre compte en fonction des paramètres de filtrage	Lecture			
DescribeFleetAdvisorLsaAnalysis	Accorde l'autorisation de renvoyer une liste paginée contenant les descriptions des analyses d'évaluation à grande échelle (LSA) produites par vos collecteurs Fleet Advisor	Lecture			
DescribeFleetAdvisorSchemaObjectSummary	Accorde l'autorisation de renvoyer une liste paginée des descriptions de schémas découvertes par vos collecteurs Fleet Advisor en fonction des paramètres de filtrage	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFleetAdvisorSchemas	Accorde l'autorisation de renvoyer une liste paginée des schémas découverts par vos collecteurs Fleet Advisor en fonction des paramètres de filtrage	Lecture			
DescribeMetadataModel	Accorde l'autorisation d'obtenir des informations détaillées sur le modèle de métadonnées spécifié, y compris sa définition et les objets convertis correspondants dans la base de données cible, le cas échéant	Lecture	Migration Project*		
DescribeMetadataModelChildren	Accorde l'autorisation d'obtenir une liste de modèles de métadonnées enfants pour le modèle de métadonnées spécifié dans la hiérarchie de base de données	Lecture	Migration Project*		
DescribeMetadataModelCreations	Accorde l'autorisation de renvoyer une liste paginée de demandes de création de modèles de métadonnées pour un projet de migration	Lecture	Migration Project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeMetadataModelImports	Accorde l'autorisation de renvoyer des informations sur les opérations d'importation du modèle de métadonnées de démarrage pour un projet de migration	Lecture	Migration Project*		
DescribeOrderableReplicationInstances	Accorde l'autorisation de renvoyer des informations sur les types d'instances de réplication qui peuvent être créés dans la région spécifiée	Lecture			
DescribePendingMaintenanceActions	Accorde l'autorisation de renvoyer des informations sur les actions de maintenance en cours	Lecture			
DescribeRecommendationLimitations	Accorde l'autorisation de renvoyer une liste paginée de descriptions des limitations pour les recommandations des moteurs cibles AWS	Lecture			
DescribeRecommendations	Octroie l'autorisation de renvoyer une liste paginée des descriptions de recommandations de moteurs cibles pour vos bases de données sources	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRefreshSchemasStatus	Accorde l'autorisation de renvoyer le statut de l' RefreshSchemas opération	Lecture	Endpoint*		
DescribeReplicationConfigs	Accorde l'autorisation de décrire les configurations de réplication.	Lecture			
DescribeReplicationInstanceTaskLogs	Accorde l'autorisation de renvoyer des informations sur les journaux de tâches pour la tâche spécifiée	Lecture	ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeReplicationInstances	Accorde l'autorisation de renvoyer des informations sur les instances de réplication de votre compte dans la région actuelle	Lecture			
DescribeReplicationSubnetGroups	Accorde l'autorisation de renvoyer des informations sur les groupes de sous-réseaux de réplication	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReplicationTableStatistics	Accorde l'autorisation de décrire les statistiques de la table de réplication.	Lecture	ReplicationConfig*		
DescribeReplicationTaskAssessmentResults	Accorde l'autorisation de renvoyer les derniers résultats d'évaluation des tâches à partir d'Amazon S3	Lecture	ReplicationTask		
DescribeReplicationTaskAssessmentRuns	Accorde l'autorisation de renvoyer une liste paginée des exécutions d'évaluation de prémigration en fonction des paramètres de filtrage	Lecture	ReplicationInstance		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTaskIndividualAssessments	Accorde l'autorisation de renvoyer une liste paginée des évaluations individuelles en fonction des paramètres de filtrage	Lecture	ReplicationTask		
			ReplicationTaskAssessmentRun		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReplicationTasks	Accorde l'autorisation de renvoyer des informations sur les tâches de réplication de votre compte dans la région actuelle	Lecture			
DescribeReplications	Accorde l'autorisation de décrire les réplications.	Lecture			
DescribeSchemas	Accorde l'autorisation de renvoyer des informations sur le schéma pour le point de terminaison spécifié	Lecture	Endpoint*		
DescribeTableStatistics	Accorde l'autorisation de renvoyer des statistiques de table concernant la tâche de migration de base de données, notamment le nom de la table, les lignes insérées, les lignes mises à jour et les lignes supprimées	Lecture	ReplicationTask*		
ExportMetadataModelAssessment	Accorde l'autorisation d'exporter l'évaluation du modèle de métadonnées spécifié	Écrire	MigrationProject		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTargetSelectionRules	Accorde l'autorisation de convertir les règles de sélection de source en leurs homologues cibles pour les opérations de conversion de schéma	Lecture	MigrationProject*		
ImportCertificate	Accorde l'autorisation de télécharger le certificat spécifié	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	Accorde l'autorisation de répertorier les attributs AWS DMS d'un fournisseur de données	Lecture			
ListExtensionPacks	Accorde l'autorisation de répertorier les attributs AWS DMS d'un pack d'extension	Lecture	MigrationProject		
ListInstanceProfiles	Accorde l'autorisation de répertorier les attributs AWS DMS pour les profils d'une instance	Lecture	InstanceProfile		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMetadataModelAssessmentActionItems [autorisation uniquement]	Accorde l'autorisation de répertorier les attributs AWS DMS pour les actions d'évaluation d'un modèle de métadonnées. Remarque. Malgré cette action requise StartMetadataModelImport, cette dernière n'autorise pas actuellement l'opération de conversion de schéma décrite	Lecture	Migration Project		dms:StartMetadataModelImport
ListMetadataModelAssessments	Accorde l'autorisation de répertorier les attributs AWS DMS pour les évaluations d'un modèle de métadonnées	Lecture	Migration Project		
ListMetadataModelConversions	Accorde l'autorisation de répertorier les attributs AWS DMS pour les conversions d'un modèle de métadonnées	Lecture	Migration Project		
ListMetadataModelExports	Accorde l'autorisation de répertorier les attributs AWS DMS pour les exportations d'un modèle de métadonnées	Lecture	Migration Project		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMigrationProjects	Accorde l'autorisation de répertorier les attributs AWS DMS pour un projet de migration. Remarque. Bien que cette action nécessite DescribeMigrationProjects et DescribeConversionConfiguration, les deux actions requises n'autorisent pas actuellement l'opération de conversion de schéma décrite	Lecture	DataProvider		dms:DescribeConversionConfiguration
			InstanceProfile		
			MigrationProject		
ListTagsForResource	Accorde l'autorisation de répertorier tous les tags d'une AWS ressource DMS	Lecture	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
ModifyDataMigration	Accorde l'autorisation de modifier la migration de base de données spécifiée.	Écrire	DataMigration*		iam:PassRole
ModifyEndpoint	Accorde l'autorisation de modifier le point de terminaison spécifié	Écrire	Endpoint*		iam:PassRole
			Certificate		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyEventSubscription	Accorde l'autorisation de modifier un abonnement existant aux notifications d'événements AWS DMS	Écrire			
ModifyFleetAdvisorCollector [autorisation uniquement]	Accorde l'autorisation de modifier le nom et la description du collecteur Fleet Advisor spécifié	Écrire			
ModifyFleetAdvisorCollectorStatuses [autorisation uniquement]	Accorde l'autorisation de modifier l'état du collecteur Fleet Advisor spécifié	Écrire			
ModifyOutboundIntegration [autorisation uniquement]	Autorise DMS à modifier les ressources pour les intégrations sans ETL avec des bases de données autogérées	Écrire			iam:PassRole
ModifyReplicationConfig	Accorde l'autorisation de modifier la configuration de réplication spécifiée.	Écrire	ReplicationConfig*		
ModifyReplicationInstance	Accorde l'autorisation de modifier l'instance de réplication pour appliquer de nouveaux paramètres	Écriture	ReplicationInstance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyReplicationSubnetGroup	Accorde l'autorisation de modifier les paramètres du groupe de sous-réseaux de réplication spécifié	Écriture			
ModifyReplicationTask	Accorde l'autorisation de modifier la tâche de réplication spécifiée	Écriture	ReplicationTask*		
MoveReplicationTask	Accorde l'autorisation de déplacer la tâche de réplication spécifiée vers une instance de réplication différente.	Écriture	ReplicationInstance* ReplicationTask*		
RebootReplicationInstance	Accorde l'autorisation de redémarrer une instance de réplication Le redémarrage entraîne une interruption momentanée, jusqu'à ce que l'instance de réplication redevienne disponible	Écriture	ReplicationInstance*		
RefreshSchemas	Accorde l'autorisation de remplir le schéma pour le point de terminaison spécifié	Écrire	Endpoint* ReplicationInstance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ReloadReplicationTables	Accorde l'autorisation de recharger la table de base de données cible avec la source d'une réplication.	Écrire	ReplicationConfig*		
ReloadTables	Accorde l'autorisation de recharger la table de base de données cible avec les données sources	Écriture	ReplicationTask*		
RemoveTagsFromResource	Accorde l'autorisation de supprimer des balises de métadonnées d'une ressource DMS	Identification	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RunFleetAdvisorLsaAnalysis	Accorde l'autorisation d'exécuter une analyse d'évaluation à grande échelle (LSA) sur chaque collecteur Fleet Advisor de votre compte	Écrire			
StartDataMigration	Accorde l'autorisation de lancer la migration de base de données.	Écrire	DataMigration*		
StartMetadataModelAssessment	Accorde l'autorisation de démarrer une nouvelle évaluation du modèle de métadonnées	Écrire	MigrationProject*		
StartMetadataModelConversion	Accorde l'autorisation de démarrer une nouvelle conversion du modèle de métadonnées	Écrire	MigrationProject*		
StartMetadataModelCreation	Accorde l'autorisation de créer un modèle de métadonnées source du type donné avec les propriétés spécifiées pour les opérations de conversion de schéma	Écrire	MigrationProject*		
StartMetadataModelExportAsScripts	Accorde l'autorisation de démarrer une nouvelle exportation du modèle de métadonnées en tant que script	Écrire	MigrationProject*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMetadataModelExportToTarget	Accorde l'autorisation de démarrer une nouvelle exportation du modèle de métadonnées vers la cible	Écrire	MigrationProject*		
StartMetadataModelImport	Accorde l'autorisation de démarrer une nouvelle importation du modèle de métadonnées	Écrire	MigrationProject*		
StartRecommendations	Octroie l'autorisation de démarrer l'analyse de votre base de données source afin de fournir des recommandations de moteurs cibles	Écrire			
StartReplication	Accorde l'autorisation de lancer une réplication.	Écrire	ReplicationConfig*		
StartReplicationTask	Accorde l'autorisation de démarrer la tâche de réplication	Écriture	ReplicationTask*		
StartReplicationTaskAssessment	Accorde l'autorisation de démarrer l'évaluation de la tâche de réplication pour les types de données non pris en charge dans la base de données source	Écriture	ReplicationTask*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartReplicationTaskAssessmentRun	Accorde l'autorisation de démarrer une nouvelle évaluation de prémigration pour une ou plusieurs évaluations individuelles d'une tâche de migration	Écrire	ReplicationTask*		iam:PassRole
StopDataMigration	Accorde l'autorisation d'arrêter la migration de base de données.	Écrire	DataMigration*		
StopReplication	Accorde l'autorisation d'arrêter une réplication.	Écrire	ReplicationConfig*		
StopReplicationTask	Accorde l'autorisation d'arrêter la tâche de réplication	Écriture	ReplicationTask*		
TestConnection	Accorde l'autorisation de tester la connexion entre l'instance de réplication et le point de terminaison	Lecture	Endpoint*		
			ReplicationInstance*		
UpdateConversionConfiguration	Accorde l'autorisation de mettre à jour une configuration de conversion	Écrire	MigrationProject*		
UpdateDataProvider	Accorde l'autorisation de mettre à jour le fournisseur de données spécifié	Écrire	DataProvider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateInstanceProfile	Accorde l'autorisation de mettre à jour le profil d'instance spécifié	Écrire	InstanceProfile*		
UpdateMigrationProject	Accorde l'autorisation de mettre à jour le projet de migration spécifié	Écrire	MigrationProject*		
UpdateSubscriptionsToEventBridge	Accorde l'autorisation de migrer les abonnements DMS sur Eventbridge	Écrire			
UploadFileMetadataList [autorisation uniquement]	Accorde l'autorisation de télécharger des fichiers vers votre compartiments Amazon S3	Écrire			

Types de ressources définis par AWS Database Migration Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Certificate	arn:${Partition}:dms:${Region}:${Account}:cert:*	aws:ResourceTag/${TagKey} dms:cert-tag/${TagKey}
DataProvider	arn:${Partition}:dms:${Region}:${Account}:data-provider:*	aws:ResourceTag/${TagKey} dms:data-provider-tag/${TagKey}
DataMigration	arn:${Partition}:dms:${Region}:${Account}:data-migration:*	aws:ResourceTag/${TagKey} dms:data-migration-tag/${TagKey}
Endpoint	arn:${Partition}:dms:${Region}:${Account}:endpoint:*	aws:ResourceTag/${TagKey} dms:endpoint-tag/${TagKey}
EventSubscription	arn:${Partition}:dms:${Region}:${Account}:es:*	aws:ResourceTag/${TagKey} dms:es-tag/${TagKey}
InstanceProfile	arn:${Partition}:dms:${Region}:${Account}:instance-profile:*	aws:ResourceTag/${TagKey} dms:instance-profile-tag/${TagKey}
MigrationProject	arn:${Partition}:dms:${Region}:${Account}:migration-project:*	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
		dms:migration-project-tag/${TagKey}
ReplicationConfig	arn:${Partition}:dms:${Region}:${Account}:replication-config:*	aws:ResourceTag/${TagKey} dms:replication-config-tag/${TagKey}
ReplicationInstance	arn:${Partition}:dms:${Region}:${Account}:rep:*	aws:ResourceTag/${TagKey} dms:rep-tag/${TagKey}
ReplicationSubnetGroup	arn:${Partition}:dms:${Region}:${Account}:subgrp:*	aws:ResourceTag/${TagKey} dms:subgrp-tag/${TagKey}
ReplicationTask	arn:${Partition}:dms:${Region}:${Account}:task:*	aws:ResourceTag/${TagKey} dms:task-tag/${TagKey}
ReplicationTaskAssessmentRun	arn:${Partition}:dms:${Region}:${Account}:assessment-run:*	aws:ResourceTag/${TagKey} dms:assessment-run-tag/${TagKey}

Types de ressources	ARN	Clés de condition
ReplicationTaskIndividualAssessment	`arn:${Partition}:dms:${Region}:${Account}:individual-assessment:*`	aws:ResourceTag/${TagKey} dms:individual-assessment-tag/${TagKey}

Clés de condition pour le Service AWS de Migration de Base de Données

AWS Database Migration Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
dms:assessment-run-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de AssessmentRun	String
dms:cert-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande de certificat	String

Clés de condition	Description	Type
dms:data-migration-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de DataMigration	String
dms:data-provider-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de DataProvider	String
dms:endpoint-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande de point de terminaison	String
dms:es-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de EventSubscription	String
dms:individual-assessment-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de IndividualAssessment	String
dms:instance-profile-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de InstanceProfile	String
dms:migration-project-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de MigrationProject	String
dms:rep-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de ReplicationInstance	String
dms:replication-config-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de ReplicationConfig	String
dms:req-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande donnée	String

Clés de condition	Description	Type
dms:subgrp-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de ReplicationSubnetGroup	String
dms:task-tag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise dans la demande de ReplicationTask	String

Actions, ressources et clés de condition pour Database Query Metadata Service

Database Query Metadata Service (préfixe de service : `dbqms`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Database Query Metadata Service
- Types de ressources définis par Database Query Metadata Service
- Clés de condition pour Database Query Metadata Service

Actions définies par Database Query Metadata Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFavoriteQuery	Accorde l'autorisation de créer une requête préférée.	Écriture			
CreateQueryHistory	Accorde l'autorisation d'ajouter une requête à l'historique.	Écriture			
CreateTab	Accorde l'autorisation de créer un onglet de requête.	Écriture			
DeleteFavoriteQueries	Accorde l'autorisation de supprimer les requêtes enregistrées.	Écriture			
DeleteQueryHistory	Accorde l'autorisation de supprimer une requête historique.	Écriture			
DeleteTab	Accorde l'autorisation de supprimer l'onglet de requête.	Écriture			
DescribeFavoriteQueries	Accorde l'autorisation de répertorier les requêtes enregistrées et les métadonnées associées.	Liste			
DescribeQueryHistory	Accorde l'autorisation de répertorier l'historique des requêtes qui ont été exécutées.	Liste			
DescribeTabs	Accorde l'autorisation de répertorier les onglets de	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	requête et les métadonnées associées.				
GetQueryString	Accorde l'autorisation de récupérer la chaîne de requête favorite ou historique par ID.	Lecture			
UpdateFavoriteQuery	Accorde l'autorisation de mettre à jour la requête et la description enregistrées.	Écriture			
UpdateQueryHistory	Accorde l'autorisation de mettre à jour l'historique des requêtes.	Écriture			
UpdateTab	Accorde l'autorisation de mettre à jour l'onglet de requête.	Écriture			

Types de ressources définis par Database Query Metadata Service

Database Query Metadata Service ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à Database Query Metadata Service, indiquez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Database Query Metadata Service

DBQMS ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS DataSync

AWS DataSync (préfixe de service :`datasync`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS DataSync
- Types de ressources définis par AWS DataSync
- Clés de condition pour AWS DataSync

Actions définies par AWS DataSync

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddStorageSystem	Accorde l'autorisation de créer un système de stockage.	Écrire	agent*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
CancelTaskExecution	Accorde l'autorisation d'annuler l'exécution d'une tâche de synchronisation	Écriture	taskexecution*		
				aws:ResourceTag/${TagKey}	
CreateAgent	Accorde l'autorisation d'activer un agent que vous avez déployé sur votre hôte	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationAzureBlob	Octroie l'autorisation de créer un point de terminaison pour un conteneur Microsoft Azure Blob Storage.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLocationEfs	Accorde l'autorisation de créer un point de terminaison pour un système de fichiers Amazon EFS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxLustre	Accorde l'autorisation de créer un point de terminaison pour un Amazon FSx for Lustre	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOntap	Accorde l'autorisation de créer un point de terminaison pour Amazon FSx for ONTAP	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOpenZfs	Accorde l'autorisation de créer un point de terminaison pour Amazon FSx pour OpenZFS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLocationFsxWindows	Accorde l'autorisation de créer un point de terminaison pour un système de fichiers Amazon FSx Windows File Server	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationHdfs	Accorde l'autorisation de créer un point de terminaison pour un Amazon Hdfs	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationNfs	Accorde l'autorisation de créer un point de terminaison pour un système de fichiers NFS	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationObjectStorage	Accorde l'autorisation de créer un point de terminaison pour un compartiment de stockage d'objets autogéré	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLocationS3	Accorde l'autorisation de créer un point de terminaison pour un compartiment Amazon S3	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationSmb	Accorde l'autorisation de créer un point de terminaison pour un système de fichiers SMB	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTask	Accorde l'autorisation de créer une tâche de synchronisation	Écrire	location* agent	aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Accorde l'autorisation de supprimer un agent	Écrire	agent*		
DeleteLocation	Accorde l'autorisation de supprimer un lieu utilisé par AWS DataSync	Écrire	location*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTask	Accorde l'autorisation de supprimer une tâche de synchronisation	Écriture	task*		
DescribeAgent	Accorde l'autorisation d'afficher des métadonnées telles que le nom, les interfaces réseau et le statut (en d'autres termes, si l'agent est en cours d'exécution ou non) sur un agent de synchronisation	Lecture	agent*		
DescribeDiscoveryJob	Accorde l'autorisation de décrire les métadonnées d'une tâche de découverte.	Lecture	discovery job*		
DescribeLocationAzureBlob	Octroie l'autorisation d'afficher des métadonnées, telles que les informations de chemin d'accès, relatives à un emplacement de synchronisation Azure Blob Storage.	Lecture	location*		
DescribeLocationEfs	Accorde l'autorisation d'afficher des métadonnées, telles que les informations de chemin d'accès à un emplacement de synchronisation Amazon EFS	Lecture	location*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeLocationFsxLustre	Accorde l'autorisation d'afficher les métadonnées, telles que les informations de chemin relatives à un emplacement de synchronisation Amazon FSx Lustre	Lecture	location*		
DescribeLocationFsxOntap	Accorde l'autorisation de consulter les métadonnées, telles que les informations de chemin relatives à un emplacement de synchronisation Amazon FSx for ONTAP	Lecture	location*		
DescribeLocationFsxOpenZfs	Accorde l'autorisation d'afficher les métadonnées, telles que les informations de chemin relatives à un emplacement de synchronisation Amazon FSx OpenZFS	Lecture	location*		
DescribeLocationFsxWindows	Accorde l'autorisation d'afficher les métadonnées, telles que les informations de chemin relatives à un emplacement de synchronisation Amazon FSx Windows	Lecture	location*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeLocationHdfs	Accorde l'autorisation d'afficher des métadonnées, telles que les informations de chemin d'accès à un emplacement de synchronisation Amazon HDFS	Lecture	location*		
DescribeLocationNfs	Accorde l'autorisation d'afficher des métadonnées, telles que les informations de chemin d'accès à un emplacement de synchronisation NFS	Lecture	location*		
DescribeLocationObjectStorage	Accorde l'autorisation d'afficher des métadonnées relatives à un emplacement de serveur de stockage d'objets autogéré	Lecture	location*		
DescribeLocationS3	Accorde l'autorisation d'afficher des métadonnées, telles que le nom du compartiment, relatives à un emplacement de synchronisation de compartiment Amazon S3	Lecture	location*		
DescribeLocationSmb	Accorde l'autorisation d'afficher des métadonnées, telles que les informations de chemin d'accès, relatives à un emplacement de synchronisation SMB	Lecture	location*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeStorageSystem	Accorde l'autorisation d'afficher des métadonnées relatives à un système de stockage.	Lecture	storagesystem*		
DescribeStorageSystemResourceMetrics	Accorde l'autorisation de décrire les métriques de ressources collectées par une tâche de découverte.	List	discoveryjob*		
DescribeStorageSystemResources	Accorde l'autorisation de décrire les ressources identifiées par une tâche de découverte.	List	discoveryjob*		
DescribeTask	Accorde l'autorisation d'afficher des métadonnées relatives à une tâche de synchronisation	Lecture	task*		
DescribeTaskExecution	Accorde l'autorisation d'afficher des métadonnées relatives à une tâche de synchronisation en cours d'exécution	Lecture	taskexecution*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations	Accorde l'autorisation de générer des recommandations pour une ressource identifiée par une tâche de découverte.	Écrire	discoveryjob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAgents	Accorde l'autorisation de répertorier les agents détenus par et Compte AWS dans une région spécifiée dans la demande	List			
ListDiscoveryJobs	Accorde l'autorisation de répertorier les tâches de découverte.	List			
ListLocations	Accorde l'autorisation de répertorier des emplacements de synchronisation source et de destination	List			
ListStorageSystems	Accorde l'autorisation de répertorier les systèmes de stockage.	List			
ListTagsForResource	Accorde l'autorisation de répertorier des balises ajoutées à la ressource spécifiée	Lecture	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTaskExecutions	Accorde l'autorisation de répertorier des tâches de synchronisation exécutées	Liste		aws:ResourceTag/${TagKey}	
ListTasks	Accorde l'autorisation de répertorier de toutes les tâches de synchronisation	List			
RemoveStorageSystem	Accorde l'autorisation de supprimer un système de stockage.	Écrire	storagesystem*		
StartDiscoveryJob	Accorde l'autorisation de lancer une tâche de découverte pour un système de stockage.	Écrire	storagesystem*		
StartTaskExecution	Accorde l'autorisation de démarrer une invocation spécifique d'une tâche de synchronisation	Écrire	task*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StopDiscoveryJob	Accorde l'autorisation d'arrêter une tâche de découverte.	Écrire	discoveryjob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'appliquer une paire clé-valeur à une ressource AWS	Identification	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises de la ressource spécifiée	Identification	agent		
			discoveryjob		
			location		
			storagesystem		
			task		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			taskexecution		
				aws:TagKeys	
UpdateAgent	Accorde l'autorisation de mettre à jour le nom d'un agent	Écrire	agent*		
UpdateDiscoveryJob	Accorde l'autorisation de mettre à jour une tâche de découverte	Écrire	discoveryjob*		
UpdateLocationAzureBlob	Octroie l'autorisation de mettre à jour un emplacement de synchronisation Azure Blob Storage.	Écrire	location*		
UpdateLocationEfs	Autorise la mise à jour d'un emplacement de synchronisation EFS	Écrire	location*		
UpdateLocationFsxLustre	Autorise la mise à jour d'un emplacement de synchronisation FSx Lustre	Écrire	location*		
UpdateLocationFsxOntap	Autorise la mise à jour d'un emplacement FSx de synchronisation ONTAP	Écrire	location*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateLocationFsxOpenZfs	Autorise la mise à jour d'un emplacement de FSx synchronisation OpenZFS	Écrire	location*		
UpdateLocationFsxWindows	Autorise la mise à jour d'un emplacement de synchronisation FSx Windows	Écrire	location*		
UpdateLocationHdfs	Accorde l'autorisation de mettre à jour un emplacement de synchronisation HDFS	Écrire	location*		
UpdateLocationNfs	Accorde l'autorisation de mettre à jour un emplacement de synchronisation NFS	Écrire	location*		
UpdateLocationObjectStorage	Accorde l'autorisation de mettre à jour un emplacement de serveur de stockage d'objets autogéré	Écrire	location*		
UpdateLocationS3	Autorise la mise à jour d'un emplacement de synchronisation S3	Écrire	location*		
UpdateLocationSmb	Accorde l'autorisation de mettre à jour un emplacement de synchronisation SMB	Écrire	location*		
UpdateStorageSystem	Accorde l'autorisation de mettre à jour un système de stockage.	Écrire	storagesystem*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTask	Accorde l'autorisation de mettre à jour des métadonnées associées à une tâche de synchronisation	Écriture	task*		
UpdateTaskExecution	Accorde l'autorisation de mettre à jour l'exécution d'une tâche de synchronisation	Écrire	taskexecution*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS DataSync

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
agent	`arn:${Partition}:datasync:${Region}:${AccountId}:agent/${AgentId}`	aws:ResourceTag/${TagKey}
location	`arn:${Partition}:datasync:${Region}:${AccountId}:location/${LocationId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
task	arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}	aws:ResourceTag/${TagKey}
taskexecution	arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}/execution/${ExecutionId}	aws:ResourceTag/${TagKey}
storagesystem	arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}	aws:ResourceTag/${TagKey}
discoveryjob	arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}/job/${DiscoveryJobId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS DataSync

AWS DataSync définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identifications associées à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtrer l'accès en fonction des clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon DataZone

Amazon DataZone (préfixe de service :`datazone`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon DataZone
- Types de ressources définis par Amazon DataZone
- Clés de condition pour Amazon DataZone

Actions définies par Amazon DataZone

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptPredictions	Accorde l'autorisation d'accepter la prédiction	Écrire			
AcceptSubscriptionRequest	Accorde l'autorisation d'approuver une demande d'abonnement pour une ressource de données	Écrire			
AddEntityOwner	Accorde l'autorisation d'ajouter un propriétaire à une entité telle qu'une unité de domaine	Écrire			
AddPolicyGrant	Accorde l'autorisation d'ajouter une subvention de politique	Gestion des autorisations			
AssociateEnvironmentRole	Accorde l'autorisation d'associer un rôle dans un environnement de plan de service par défaut	Écrire			
AssociateGovernedTerms	Accorde l'autorisation d'associer des termes régis à un actif	Écrire			
BatchDeleteLinkedTypes [autorisation uniquement]	Accorde l'autorisation de supprimer des éléments de type lié d'un DataZone domaine Amazon	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetAttributesMetadata	Accorde l'autorisation de récupérer les métadonnées des attributs	Lecture			
BatchGetCell	Accorde l'autorisation d'obtenir des cellules par lots	Lecture			
BatchGetCellRun	Accorde l'autorisation d'obtenir des analyses de cellules par lots	Lecture			
BatchPutAttributesMetadata	Accorde l'autorisation de créer et de mettre à jour les métadonnées des attributs	Écrire			
BatchPutLinkedTypes [autorisation uniquement]	Accorde l'autorisation de placer des éléments de type lié à un DataZone domaine Amazon	Écrire	domain*		
CancelMetadataGenerationRun	Autorise l'annulation de l'exécution de génération de métadonnées	Écrire			
CancelSubscription	Accorde l'autorisation de révoquer ou d'annuler un abonnement approuvé à une ressource de données	Écrire			
CreateAccountPool	Accorde l'autorisation de créer un pool de comptes	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAsset	Accorde l'autorisation de créer une ressource	Écrire			
CreateAssetFilter	Accorde l'autorisation de créer un filtre d'actifs	Écrire			
CreateAssetRevision	Accorde l'autorisation de créer une nouvelle révision d'une ressource	Écrire			
CreateAssetType	Accorde l'autorisation de créer un type de ressource	Écrire			
CreateCell	Accorde l'autorisation de créer des cellules	Écrire			
CreateCellRun	Accorde l'autorisation de créer des séries de cellules	Écrire			
CreateConnection	Accorde l'autorisation de créer des connexions	Écrire			
CreateDataProduct	Accorde l'autorisation de créer un produit de données	Écrire			
CreateDataProductRevision	Accorde l'autorisation de créer une révision du produit de données	Écrire			
CreateDataSource	Accorde l'autorisation de créer un nouveau DataSource	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDomain	Accorde l'autorisation de fournir un domaine qui est une entité de premier niveau contenant d'autres DataZone ressources Amazon	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomainUnit	Accorde l'autorisation de créer une unité de domaine	Écrire			
CreateEnvironment	Accorde l'autorisation de créer une collection de ressources configurées utilisée pour publier des données et s'y abonner	Écrire			
CreateEnvironmentAction	Accorde l'autorisation de créer une action environnementale dans un environnement de plan de service par défaut	Écrire			
CreateEnvironmentBlueprint	Accorde l'autorisation de créer un plan d'environnement personnalisé qui permet à l'utilisateur d'ajouter des environnements à son projet	Écrire			
CreateEnvironmentProfile	Accorde l'autorisation de créer un modèle à partir d'un plan qui peut être utilisé pour créer un environnement	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFormType	Accorde l'autorisation de créer un type de formulaire ou une nouvelle révision de celui-ci	Écrire			
CreateGlossary	Accorde l'autorisation de créer un nouveau glossaire métier	Écrire			
CreateGlossaryTerm	Accorde l'autorisation de créer un terme de glossaire	Écrire			
CreateGroupProfile	Accorde l'autorisation de créer un profil de DataZone groupe pour un groupe IAM Identity Center	Écrire			
CreateListingChangeSet	Accorde l'autorisation de créer un ensemble de modifications de liste	Écrire			
CreateNotebook	Accorde l'autorisation de créer des blocs-notes	Écrire			
CreateProject	Accorde l'autorisation de créer un projet afin de permettre à votre équipe de publier des données et de s'y abonner	Écrire			
CreateProjectMembership	Accorde l'autorisation d'ajouter un utilisateur à un projet	Écrire			
CreateProjectProfile	Accorde l'autorisation de créer un profil de projet	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRule	Accorde l'autorisation de créer une règle	Écrire			
CreateSubscriptionGrant	Accorde l'autorisation de créer un octroi pour un abonnement approuvé sur une cible d'abonnement	Écrire			
CreateSubscriptionRequest	Accorde l'autorisation de créer une demande abonnement pour une ressource de données	Écrire			
CreateSubscriptionTarget	Accorde l'autorisation de créer une cible d'abonnement pour un environnement du projet	Écrire			
CreateUserProfile	Accorde l'autorisation de créer un profil utilisateur pour un utilisateur existant dans IAM Identity Center	Écrire			
DeleteAccountPool	Accorde l'autorisation de supprimer un pool de comptes	Écrire			
DeleteAsset	Accorde l'autorisation de supprimer une ressource	Écrire			
DeleteAssetFilter	Accorde l'autorisation de supprimer le filtre de ressources	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAssetType	Accorde l'autorisation de supprimer un type de ressource	Écrire			
DeleteCell	Accorde l'autorisation de supprimer des cellules	Écrire			
DeleteCellRun	Accorde l'autorisation de supprimer des séries de cellules	Écrire			
DeleteConnection	Accorde l'autorisation de supprimer des connexions	Écrire			
DeleteDataExportConfiguration	Accorde l'autorisation de supprimer la configuration d'exportation des données du DataZone catalogue	Écrire			
DeleteDataProduct	Accorde l'autorisation de supprimer le produit de données	Écrire			
DeleteDataSource	Autorise la mise à jour des données existantes DataSource	Écrire			
DeleteDomain	Accorde l'autorisation de supprimer un domaine provisionné	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDomainSharingPolicy [autorisation uniquement]	Accorde l'autorisation de supprimer une politique de ressources pour un DataZone domaine	Gestion des autorisations			
DeleteDomainUnit	Autorise la suppression d'une unité de domaine existante	Écrire			
DeleteEnvironment	Accorde l'autorisation de supprimer un environnement	Écrire			
DeleteEnvironmentAction	Accorde l'autorisation de supprimer une action environnementale dans un environnement de plan de service par défaut	Écrire			
DeleteEnvironmentBlueprint	Accorde l'autorisation de supprimer un plan d'environnement	Écrire			
DeleteEnvironmentBlueprintConfiguration	Accorde l'autorisation de supprimer une configuration de plan d'environnement	Écrire			
DeleteEnvironmentProfile	Accorde l'autorisation de supprimer un profil d'environnement	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFormType	Accorde l'autorisation de supprimer un type de formulaire	Écrire			
DeleteGlossary	Accorde l'autorisation de supprimer un glossaire métier	Écrire			
DeleteGlossaryTerm	Accorde l'autorisation de supprimer un terme de glossaire	Écrire			
DeleteListing	Accorde l'autorisation de supprimer une liste	Écrire			
DeleteNotebook	Accorde l'autorisation de supprimer des blocs-notes	Écrire			
DeleteProject	Accorde l'autorisation de supprimer un projet qui permet à votre équipe de publier des données et de s'y abonner	Écrire			
DeleteProjectMembership	Accorde l'autorisation de supprimer un utilisateur d'un projet	Écrire			
DeleteProjectProfile	Accorde l'autorisation de supprimer un profil de projet	Écrire			
DeleteRule	Accorde l'autorisation de supprimer la règle	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSubscriptionGrant	Accorde l'autorisation de supprimer un octroi d'abonnement d'une cible d'abonnement	Écrire			
DeleteSubscriptionRequest	Accorde l'autorisation de supprimer une demande d'abonnement en attente pour une ressource de données	Écrire			
DeleteSubscriptionTarget	Accorde l'autorisation de supprimer une cible d'abonnement d'un environnement du projet	Écrire			
DeleteTimeSeriesDataPoints	Accorde l'autorisation de supprimer des fichiers existants TimeSeriesDataPoints	Écrire			
DisassociateEnvironmentRole	Accorde l'autorisation de dissocier un rôle dans un environnement de plan de service par défaut	Écrire			
DisassociateGovernedTerms	Accorde l'autorisation de dissocier les termes régis d'un actif	Écrire			
GenerateCode	Accorde l'autorisation de générer du code	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountPool	Accorde l'autorisation d'obtenir les détails du pool de comptes	Lecture			
GetAsset	Accorde l'autorisation de récupérer une ressource	Lecture			
GetAssetFilter	Accorde l'autorisation d'obtenir le filtre des actifs	Lecture			
GetAssetType	Accorde l'autorisation d'obtenir un type de ressource	Lecture			
GetCell	Accorde l'autorisation d'obtenir des cellules	Lecture			
GetCellRun	Donne l'autorisation d'utiliser des téléphones portables	Lecture			
GetCellRunResult	Accorde l'autorisation d'obtenir le résultat de l'analyse cellulaire	Lecture			
GetConnection	Accorde l'autorisation d'établir des connexions	Lecture			
GetConversation	Accorde l'autorisation d'engager des conversations	Lecture			
GetDataExportConfiguration	Accorde l'autorisation de récupérer la configuration d'exportation des données du DataZone catalogue	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataProduct	Accorde l'autorisation d'obtenir un produit de données	Lecture			
GetDataSource	Autorise Get a existing DataSource in Amazon à DataZone l'aide de son identifiant	Lecture			
GetDataSourceRun	Accorde l'autorisation d' DataSource exécuter une tâche sur Amazon en DataZone utilisant son identifiant	Lecture			
GetDomain	Accorde l'autorisation de récupérer des informations sur un domaine	Lecture	domain*		
GetDomainExecutionRoleCredentials [autorisation uniquement]	Accorde l'autorisation d'utiliser les fonctionnalités qui nécessitent l'accès aux informations d'identification du rôle d'exécution du domaine	Lecture			
GetDomainSharingPolicy [autorisation uniquement]	Accorde l'autorisation de récupérer une politique de ressources pour un DataZone domaine	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDomainUnit	Accorde l'autorisation d'obtenir une unité de domaine existante	Lecture			
GetEnvironment	Accorde l'autorisation d'obtenir les détails d'un environnement	Lecture			
GetEnvironmentAction	Accorde l'autorisation d'effectuer une action environnementale dans un environnement de plan de service par défaut	Lecture			
GetEnvironmentActionLink [autorisation uniquement]	Accorde l'autorisation d'obtenir un lien d'action d'environnement	Lecture			
GetEnvironmentBlueprint	Accorde l'autorisation d'obtenir les détails d'un plan d'environnement	Lecture			
GetEnvironmentBlueprintConfiguration	Accorde l'autorisation d'obtenir la configuration d'un plan d'environnement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEnvironmentCredentials	Accorde l'autorisation d'obtenir des informations d'identification temporaires associées au rôle d'utilisateur de l'environnement	Lecture			
GetEnvironmentProfile	Accorde l'autorisation d'obtenir les détails du profil d'environnement	Lecture			
GetFormType	Accorde l'autorisation d'obtenir un type de formulaire	Lecture			
GetGlossary	Accorde l'autorisation d'obtenir un glossaire métier	Lecture			
GetGlossaryTerm	Accorde l'autorisation d'obtenir un terme du glossaire	Lecture			
GetGroupProfile	Accorde l'autorisation de récupérer un profil de DataZone groupe existant	Lecture			
GetIamPortalLoginUrl	Autorise un directeur IAM à se connecter au portail DataZone	Gestion des autorisations			
GetJobRun	Donne l'autorisation d'exécuter des tâches	Lecture			
GetLineageEvent	Accorde l'autorisation d'obtenir des événements de lignage	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLineageNode	Accorde l'autorisation d'obtenir le nœud de lignée	Lecture			
GetListing	Accorde l'autorisation d'obtenir une liste	Lecture			
GetMetadataGenerationRun	Octroie l'autorisation d'obtenir l'exécution de génération des métadonnées.	Lecture			
GetNotebook	Accorde l'autorisation d'obtenir des blocs-notes	Lecture			
GetNotebookCompute	Accorde l'autorisation d'accéder à un ordinateur portable	Lecture			
GetNotebookExport	Accorde l'autorisation d'exporter des blocs-notes	Lecture			
GetProject	Accorde l'autorisation d'obtenir les détails du projet	Lecture			
GetProjectProfile	Accorde l'autorisation d'obtenir les détails du profil du projet	Lecture			
GetRule	Accorde l'autorisation d'obtenir une règle	Lecture			
GetSubscription	Accorde l'autorisation de récupérer un abonnement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSubscriptionEligibility [autorisation uniquement]	Accorde l'autorisation d'obtenir l'éligibilité à un abonnement	Lecture			
GetSubscriptionGrant	Accorde l'autorisation de récupérer un octroi d'abonnement	Lecture			
GetSubscriptionRequestDetails	Accorde l'autorisation de rejeter une demande d'abonnement pour une ressource de données	Lecture			
GetSubscriptionTarget	Accorde l'autorisation de récupérer les détails d'une cible d'abonnement	Lecture			
GetTimeSeriesDataPoint	Accorde l'autorisation d'obtenir un objet existant sur Amazon TimeSeriesDataPoints à DataZone l'aide de son identifiant	Lecture			
GetUpdateEligibility	Accorde l'autorisation d'obtenir une mise à jour du statut d'éligibilité pour les constructions de projets	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetUserProfile	Accorde l'autorisation de récupérer un profil utilisateur pour un utilisateur existant dans le DataZone domaine	Lecture			
ListAccountEnvironments	Accorde l'autorisation de répertorier les environnements dans tous les domaines d'un AWS compte	List			
ListAccountPools	Accorde l'autorisation de répertorier les pools de comptes	List			
ListAccountsInAccountPool	Accorde l'autorisation de répertorier des comptes dans un pool de comptes	List			
ListAssetFilters	Accorde l'autorisation de répertorier les filtres d'actifs	List			
ListAssetRevisions	Accorde l'autorisation de répertorier les révisions d'une ressource	List			
ListCellRuns	Accorde l'autorisation de répertorier les séries de cellules	List			
ListConnections	Accorde l'autorisation de répertorier les connexions	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConversations	Octroie l'autorisation de répertorier les conversations.	List			
ListDataProductRevisions	Accorde l'autorisation de répertorier les révisions des produits de données	List			
ListDataSourceRunActivities	Accorde l'autorisation de DataSource répertorier les activités des tâches sur Asset	List			
ListDataSourceRuns	Accorde l'autorisation de lister les DataSource exécutions de tâches	List			
ListDataSources	Accorde l'autorisation de répertorier des objets existants DataSources	List			
ListDomainUnitsForParent	Accorde l'autorisation de répertorier les unités de domaine enfant pour une unité de domaine parent donnée	List			
ListDomains	Accorde l'autorisation de récupérer tous les domaines	List			
ListEntityOwners	Accorde l'autorisation de répertorier les propriétaires d'une entité telle qu'une unité de domaine	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEnvironmentActions	Accorde l'autorisation de répertorier les actions environnementales dans un environnement de plan de service par défaut	List			
ListEnvironmentBlueprintConfigurationSummaries [autorisation uniquement]	Accorde l'autorisation de répertorier les résumés de configuration du plan d'environnement	List			
ListEnvironmentBlueprintConfigurations	Accorde l'autorisation de répertorier les configurations de plan d'environnement	List			
ListEnvironmentBlueprints	Accorde l'autorisation de répertorier les domaines pour les plans d'environnement	List			
ListEnvironmentProfiles	Accorde l'autorisation de répertorier les domaines pour les profils d'environnement	List			
ListEnvironments	Accorde l'autorisation d'afficher les environnements du domaine	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGroupsForUser	Accorde l'autorisation de répertorier tous les profils de DataZone groupe dont le profil DataZone utilisateur est membre	List			
ListJobRuns	Accorde l'autorisation de répertorier les exécutions de tâches	List			
ListLineageEvents	Accorde l'autorisation de répertorier les événements de lignage	List			
ListLineageNodeHistory	Accorde l'autorisation de répertorier les versions historiques du nœud de lignée	List			
ListLinkedTypes [autorisation uniquement]	Accorde l'autorisation de répertorier les articles de type lié liés à un DataZone domaine Amazon	List	domain*		
ListMetadataGenerationRuns	Octroie l'autorisation de répertorier les exécutions de génération des métadonnées.	List			
ListNotebooks	Autorise la mise en vente de blocs-notes	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNotifications	Accorde l'autorisation de répertorier les notifications et les événements d'un utilisateur DataZone	List			
ListPolicyGrants	Accorde l'autorisation de répertorier les subventions politiques	List			
ListProjectMemberships	Accorde l'autorisation de répertorier les membres d'un projet	List			
ListProjectProfiles	Accorde l'autorisation de répertorier les profils de projet	List			
ListProjects	Accorde l'autorisation de répertorier les projets	List			
ListRules	Accorde l'autorisation de répertorier les règles	List			
ListSubscriptionGrants	Accorde l'autorisation de répertorier les octrois d'abonnement pour un principal abonné	List			
ListSubscriptionRequests	Accorde l'autorisation de répertorier les demandes d'abonnement	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSubscriptionTargets	Accorde l'autorisation de répertorier les cibles d'abonnement	List			
ListSubscriptions	Accorde l'autorisation de répertorier les abonnements	List			
ListTagsForResource	Accorde l'autorisation de récupérer toutes les balises associées à une ressource.	Lecture	domain		
ListTimeSeriesDataPoints	Accorde l'autorisation de répertorier des objets existants TimeSeriesDataPoints	List			
ListWarehouseMetadata [autorisation uniquement]	Accorde l'autorisation de répertorier les secrets Manager Secrets disponibles	List			
PostLineageEvent	Accorde l'autorisation de publier des événements de lignage	Écrire			
PostTimeSeriesDataPoints	Accorde l'autorisation de publier un nouveau TimeSeriesDataPoints	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ProvisionDomain [autorisation uniquement]	Accorde l'autorisation de provisionner le domaine avec la configuration de projet par défaut	Écrire			
PutCellRunResult	Accorde l'autorisation de publier les résultats d'une analyse cellulaire	Écrire			
PutDataExportConfiguration	Accorde l'autorisation de créer et de mettre à jour la configuration d'exportation des données du DataZone catalogue	Écrire			
PutDomainSharingPolicy [autorisation uniquement]	Accorde l'autorisation d'ajouter une politique de ressources pour un DataZone domaine	Gestion des autorisations			
PutEnvironmentBlueprintConfiguration	Accorde l'autorisation de sélectionner une configuration de plan d'environnement	Écrire			
QueryGraph	Accorde l'autorisation d'interroger le graphe	List			
RefreshToken [autorisation uniquement]	Accorde l'autorisation d'actualiser un jeton	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RejectPredictions	Accorde l'autorisation de rejeter la prédiction	Écrire			
RejectSubscriptionRequest	Accorde l'autorisation de rejeter une demande d'abonnement pour une ressource de données	Écrire			
RemoveEntityOwner	Accorde l'autorisation de supprimer le propriétaire existant d'une entité telle qu'une unité de domaine	Écrire			
RemovePolicyGrant	Accorde l'autorisation de supprimer une subvention de politique	Gestion des autorisations			
RevokeSubscription	Accorde l'autorisation de révoquer un abonnement	Gestion des autorisations			
Search	Accorde l'autorisation de rechercher des entités DataZone	List			
SearchGroupProfiles	Accorde l'autorisation de rechercher des profils de DataZone groupe et des groupes IAM Identity Center	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchListings	Accorde l'autorisation de rechercher des listes	List			
SearchRules [autorisation uniquement]	Autorise les règles de recherche	List			
SearchTypes	Accorde l'autorisation de rechercher des types tels que des types de ressources et des types de formulaires dans un domaine	List			
SearchUserProfiles	Autorise la recherche de profils DataZone d'utilisateurs, d'utilisateurs d'IAM Identity Center et de profils DataZone principaux IAM	List			
SendMessage	Accorde l'autorisation d'envoyer des messages	Écrire			
SsoLogin [autorisation uniquement]	Accorde l'autorisation de se connecter via l'authentification SSO	Écrire			
SsoLogout [autorisation uniquement]	Accorde l'autorisation de se déconnecter en tant qu'utilisateur SSO	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartAccountBootstrapAction [autorisation uniquement]	Autorise le lancement d'une action de démarrage du compte pour un domaine	Écrire			
StartConversation	Autorise le lancement de conversations	Écrire			
StartDataSourceRun	Accorde l'autorisation de démarrer une tâche d' DataSource exécution	Écrire			
StartMetadataGenerationRun	Octroie l'autorisation de démarrer l'exécution de génération des métadonnées.	Écrire			
StartNotebookCompute	Accorde l'autorisation de démarrer le calcul du bloc-notes	Écrire			
StartNotebookExport	Autorise l'exportation de blocs-notes	Écrire			
StartNotebookImport	Autorise l'importation de blocs-notes	Écrire			
StopMetadataGenerationRun	Octroie l'autorisation d'interrompre l'exécution de génération des métadonnées.	Écrire			
StopNotebookCompute	Autorise l'arrêt du calcul du bloc-notes	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Octroie l'autorisation d'ajouter ou de mettre à jour des balises d'une ressource	Identification	domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises associées à une ressource.	Identification	domain*		
				aws:TagKeys	
UpdateAccountPool	Autorise la mise à jour d'un pool de comptes	Écrire			
UpdateAssetFilter	Autorise la mise à jour du filtre d'actifs	Écrire			
UpdateCell	Autorise la mise à jour des cellules	Écrire			
UpdateCellRun	Autorise la mise à jour des séries de cellules	Écrire			
UpdateConnection	Accorde l'autorisation de mettre à jour les connexions	Écrire			
UpdateDataSource	Autorise la mise à jour des données existantes DataSource	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataSourceRunActivities [autorisation uniquement]	Accorde l'autorisation de mettre à jour les activités exécutées par la source de données	Écrire			
UpdateDomain	Accorde l'autorisation de mettre à jour les informations d'un domaine	Écrire	domain*		
UpdateDomainUnit	Autorise la mise à jour d'une unité de domaine existante	Écrire			
UpdateEnvironment	Accorde l'autorisation de mettre à jour les paramètres d'un environnement	Écrire			
UpdateEnvironmentAction	Accorde l'autorisation de mettre à jour une action environnementale dans un environnement de plan de service par défaut	Écrire			
UpdateEnvironmentBlueprint	Accorde l'autorisation de mettre à jour les paramètres d'un plan d'environnement	Écrire			
UpdateEnvironmentConfiguration [autorisation uniquement]	Accorde l'autorisation de mettre à jour une configuration d'environnement	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEnvironmentDeploymentStatus [autorisation uniquement]	Accorde l'autorisation de mettre à jour le statut du déploiement de l'environnement	Écrire			
UpdateEnvironmentProfile	Accorde l'autorisation de mettre à jour EnvironmentProfile la configuration	Écrire			
UpdateGlossary	Accorde l'autorisation de mettre à jour un glossaire métier	Écrire			
UpdateGlossaryTerm	Accorde l'autorisation de mettre à jour un terme de glossaire	Écrire			
UpdateGroupProfile	Accorde l'autorisation de mettre à jour le profil d'un DataZone groupe	Écrire			
UpdateNotebook	Autorise la mise à jour des blocs-notes	Écrire			
UpdateProject	Accorde l'autorisation de mettre à jour un projet qui permet à votre équipe de publier des données et de s'y abonner	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateProjectProfile	Autorise la mise à jour d'un profil de projet	Écrire			
UpdateRule	Accorde l'autorisation de mettre à jour la règle	Écrire			
UpdateSubscriptionGrantStatus	Accorde l'autorisation de mettre à jour le statut d'un octroi d'abonnement pour les octrois personnalisés	Écrire			
UpdateSubscriptionRequest	Autorise la mise à jour de la raison métier d'une demande d'abonnement pour une ressource de données	Écrire			
UpdateSubscriptionTarget	Accorde l'autorisation de mettre à jour une cible d'abonnement	Écrire			
UpdateUserProfile	Accorde l'autorisation de mettre à jour un profil DataZone utilisateur	Écrire			
ValidatePassRole [autorisation uniquement]	Accorde l'autorisation de valider une transmission de rôle	Écrire			

Types de ressources définis par Amazon DataZone

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:datazone:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon DataZone

Amazon DataZone définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Clés de condition	Description	Type
datazone:domainId	Filtre l'accès en fonction de l'ID de domaine transmis dans la demande	String
datazone:projectId	Filtre l'accès en fonction de l'ID de projet transmis dans la demande	String
datazone:userId	Filtre l'accès en fonction de l'ID utilisateur transmis dans la demande	String

Actions, ressources et clés de condition pour AWS Deadline Cloud

AWS Deadline Cloud (préfixe de service :`deadline`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Deadline Cloud
- Types de ressources définis par AWS Deadline Cloud
- Clés de condition pour AWS Deadline Cloud

Actions définies par AWS Deadline Cloud

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateMemberToFarm	Permet d'associer un membre à une ferme	Gestion des autorisations	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToFleet	Accorde l'autorisation d'associer un membre à une flotte	Gestion des autorisations	fleet*		identitystore:DescribeGroup identitystore:DescribeUser

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToJob	Accorde l'autorisation d'associer un membre à une tâche	Gestion des autorisations	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToQueue	Accorde l'autorisation d'associer un membre à une file d'attente	Gestion des autorisations	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssumeFleetRoleForRead	Accorde l'autorisation d'assumer un rôle de flotte pour un accès en lecture seule	Écrire	fleet*		identitystore:ListGroupMembershipsForMember
AssumeFleetRoleForWorker	Autorise un travailleur à assumer un rôle dans la flotte	Écrire	worker*		
AssumeQueueRoleForRead	Accorde l'autorisation d'assumer un rôle de file d'attente pour un accès en lecture seule	Écrire	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForUser	Accorde l'autorisation d'assumer un rôle de file d'attente pour un utilisateur	Écrire	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForWorker	Accorde l'autorisation d'assumer un rôle de file d'attente pour un travailleur	Écrire	queue* worker*		
BatchGetJobEntity	Accorde l'autorisation d'obtenir une entité de travail pour un travailleur	Lecture	worker*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CopyJobTemplate	Accorde l'autorisation de copier un modèle de tâche dans un compartiment Amazon S3	Écrire	job*		identitystore:ListGroupMembershipsForMember s3:PutObject
CreateBudget	Accorde l'autorisation de créer un budget	Écrire	budget*		deadline:TagResource identitystore:ListGroupMembershipsForMember
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFarm	Accorde l'autorisation de créer une ferme	Écrire	farm*		deadline:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFleet	Accorde l'autorisation de créer une flotte	Écrire	fleet*		deadline:TagResource ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Accorde l'autorisation de créer une tâche.	Écrire	job*		deadline:GetJobTemplate identitystore:ListGroupMembershipsForMember
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLicenseEndpoint	Accorde l'autorisation de créer un point de terminaison de licence pour les logiciels ou produits sous licence	Écrire	license-endpoint*		deadline:TagResource ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLimit	Accorde l'autorisation de créer une limite pour une ferme	Écrire	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMonitor	Accorde la permission de créer un moniteur	Écrire	monitor*		deadline:TagResource iam:PassRole sso:CreateApplication sso:DeleteApplication sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Accorde l'autorisation de créer une file d'attente	Écrire	queue*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateQueueEnvironment	Accorde l'autorisation de créer un environnement de file d'attente	Écrire	queue*		identitystore:ListGroupMembershipsForMember
CreateQueueFleetAssociation	Autorise la création d'une association de flottes de files d'attente	Écrire	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateQueueLimitAssociation	Accorde l'autorisation de créer une association de limite de file d'attente	Écrire	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateStorageProfile	Accorde l'autorisation de créer un profil de stockage pour une ferme	Écrire	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorker	Accorde l'autorisation de créer un employé	Écrire	worker*		deadline:ListTagsForResource deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBudget	Autorise la suppression d'un budget	Écrire	budget*		identitystore:ListGroupMembershipsForMember
DeleteFarm	Autorise la suppression d'une ferme	Écrire	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFleet	Accorde l'autorisation de supprimer une flotte	Écrire	fleet*		identitystore:ListGroupMembershipsForMember
DeleteLicenseEndpoint	Accorde l'autorisation de supprimer un point de terminaison de licence	Écrire	license-endpoint*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteLimit	Accorde l'autorisation de supprimer une limite	Écrire	farm*		identitystore:ListGroupMembershipsForMember
DeleteMeteredProduct	Autorise la suppression d'un produit mesuré	Écrire	license-endpoint*		
DeleteMonitor	Accorde la permission de supprimer un moniteur	Écrire	monitor*		sso:DeleteApplication
DeleteQueue	Accorde l'autorisation de supprimer une file d'attente	Écrire	queue*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteQueueEnvironment	Accorde l'autorisation de supprimer un environnement de file d'attente	Écrire	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueFleetAssociation	Autorise la suppression d'une association de flottes de files d'attente	Écrire	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteQueueLimitAssociation	Accorde l'autorisation de supprimer une association de limite de file d'attente	Écrire	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteStorageProfile	Autorise la suppression d'un profil de stockage	Écrire	farm*		identitystore:ListGroupMembershipsForMember
DeleteWorker	Accorde l'autorisation de supprimer un employé	Écrire	worker*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateMemberFromFarm	Permet de dissocier un membre d'une ferme	Gestion des autorisations	farm*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromFleet	Permet de dissocier un membre d'une flotte	Gestion des autorisations	fleet*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromJob	Accorde l'autorisation de dissocier un membre d'une tâche	Gestion des autorisations	job*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateMemberFromQueue	Accorde l'autorisation de dissocier un membre d'une file d'attente	Gestion des autorisations	queue*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
GetApplicationVersion [autorisation uniquement]	Accorde l'autorisation d'obtenir la dernière version d'une application	Lecture	monitor*		
GetBudget	Donne l'autorisation d'obtenir un budget	Lecture	budget*		identitystore:ListGroupMembershipsForMember
GetFarm	Donne l'autorisation d'acquérir une ferme	Lecture	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFleet	Donne l'autorisation d'acquérir une flotte	Lecture	fleet*		identitystore:ListGroupMembershipsForMember
GetJob	Donne l'autorisation de trouver un emploi	Lecture	job*		identitystore:ListGroupMembershipsForMember
GetJobTemplate [autorisation uniquement]	Accorde l'autorisation de lire le modèle de travail	Lecture	job*		
GetLicenseEndpoint	Accorde l'autorisation d'obtenir un point de terminaison de licence	Lecture	license-endpoint*		
GetLimit	Accorde l'autorisation d'obtenir une limite	Lecture	farm*		identitystore:ListGroupMembershipsForMember
GetMonitor	Donne l'autorisation d'obtenir un moniteur	Lecture	monitor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQueue	Accorde l'autorisation d'obtenir une file d'attente	Lecture	queue*		identitystore:ListGroupMembershipsForMember
GetQueueEnvironment	Accorde l'autorisation d'obtenir un environnement de file d'attente	Lecture	queue*		identitystore:ListGroupMembershipsForMember
GetQueueFleetAssociation	Donne l'autorisation de créer une association de flottes de files d'attente	Lecture	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
GetQueueLimitAssociation	Accorde l'autorisation d'obtenir une association de limite de file d'attente	Lecture	farm*		identitystore:ListGroupMembershipsForMember
			queue*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSession	Accorde l'autorisation d'obtenir une session pour une tâche	Lecture	job*		identitystore:ListGroupMembershipsForMember
GetSessionAction	Accorde l'autorisation d'obtenir une action de session pour une tâche	Lecture	job*		identitystore:ListGroupMembershipsForMember
GetSessionsStatisticsAggregation	Autorise l'accès à toutes les statistiques collectées pour les sessions	Lecture	farm*		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		
GetStep	Accorde l'autorisation d'accéder à un emploi	Lecture	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStorageProfile	Accorde l'autorisation d'obtenir un profil de stockage	Lecture	farm*		identitystore:ListGroupMembershipsForMember
GetStorageProfileForQueue	Accorde l'autorisation d'obtenir un profil de stockage pour une file d'attente	Lecture	queue*		identitystore:ListGroupMembershipsForMember
GetTask	Accorde l'autorisation d'obtenir une tâche	Lecture	job*		identitystore:ListGroupMembershipsForMember
GetWorker	Accorde l'autorisation d'obtenir un employé	Lecture	worker*		identitystore:ListGroupMembershipsForMember
ListAvailableMeteredProducts	Accorde l'autorisation de répertorier tous les produits mesurés disponibles dans un point de terminaison de licence	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBudgets	Permet de répertorier tous les budgets d'une ferme	List	budget		identitystore:ListGroupMembershipsForMember
ListFarmMembers	Permet de répertorier tous les membres d'une ferme	List	farm*		identitystore:ListGroupMembershipsForMember
ListFarms	Donne l'autorisation de répertorier toutes les fermes	List	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListFleetMembers	Permet de répertorier tous les membres d'une flotte	List	fleet*		identitystore:ListGroupMembershipsForMember
ListFleets	Accorde l'autorisation de répertorier toutes les flottes	List	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListJobMembers	Accorde l'autorisation de répertorier tous les membres d'une offre d'emploi	List	job*		identitystore:ListGroupMembershipsForMember
ListJobParameterDefinitions	Accorde l'autorisation d'obtenir les définitions des paramètres d'une tâche dans le modèle de tâche	List	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListJobs	Accorde l'autorisation de répertorier toutes les tâches d'une file d'attente	List	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListLicenseEndpoints	Accorde l'autorisation de répertorier tous les points de terminaison de licence	List	license-endpoint*		
ListLimits	Permet de répertorier toutes les limites d'une ferme	List	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMeteredProducts	Accorde l'autorisation de répertorier tous les produits mesurés dans un point de terminaison de licence	List	license-endpoint*		
ListMonitors	Permet de répertorier tous les moniteurs	List	monitor*		
ListQueueEnvironments	Accorde l'autorisation de répertorier tous les environnements de file d'attente auxquels une file d'attente est associée	List	queue*		identitystore:ListGroupMembershipsForMember
ListQueueFleetAssociations	Permet de répertorier toutes les associations de flottes de files d'attente	List	farm*		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		
ListQueueLimitAssociations	Accorde l'autorisation de répertorier toutes les associations de limite de file d'attente	List	farm*		identitystore:ListGroupMembershipsForMember
			queue		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListQueueMembers	Permet de répertorier tous les membres d'une file	List	queue		identitystore:ListGroupMembershipsForMember
ListQueues	Permet de répertorier toutes les files d'attente d'une ferme	List	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSessionActions	Accorde l'autorisation de répertorier toutes les actions de session pour une tâche	List	job*		identitystore:ListGroupMembershipsForMember
ListSessions	Accorde l'autorisation de répertorier toutes les sessions associées à une tâche	List	job*		identitystore:ListGroupMembershipsForMember
ListSessionsForWorker	Accorde l'autorisation de répertorier toutes les sessions d'un collaborateur	List	worker		identitystore:ListGroupMembershipsForMember
ListStepConsumers	Accorde l'autorisation de répertorier les consommateurs d'étapes pour une étape de travail	List	job*		identitystore:ListGroupMembershipsForMember
ListStepDependencies	Accorde l'autorisation de répertorier les dépendances pour une étape de travail	List	job		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSteps	Accorde l'autorisation de répertorier toutes les étapes d'une tâche	List	job*		identitystore:ListGroupMembershipsForMember
ListStorageProfiles	Accorde l'autorisation de répertorier tous les profils de stockage d'une batterie de serveurs	List	farm*		identitystore:ListGroupMembershipsForMember
ListStorageProfilesForQueue	Accorde l'autorisation de répertorier tous les profils de stockage dans une file d'attente	List	queue		identitystore:ListGroupMembershipsForMember
ListTagsForResource	Accorde l'autorisation de répertorier tous les tags des ressources Deadline Cloud spécifiées	Lecture	budget		
			farm		
			fleet		
			job		
			license-endpoint		
			monitor		
			queue		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			worker		
				deadline:CalledAction	
ListTasks	Accorde l'autorisation de répertorier toutes les tâches associées à une tâche	List	job*		identitystore:ListGroupMembershipsForMember
ListWorkers	Permet de répertorier tous les travailleurs d'une flotte	List	worker*		identitystore:ListGroupMembershipsForMember
PutMeteredProduct	Accorde l'autorisation d'ajouter un produit mesuré à un point de terminaison de licence	Écrire	license-endpoint*		
SearchJobs	Autorise la recherche d'emplois dans plusieurs files d'attente	Lecture	queue*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchSteps	Accorde l'autorisation de rechercher les étapes d'une même tâche ou de rechercher dans les étapes de plusieurs files d'attente	Lecture	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchTasks	Accorde l'autorisation de rechercher les tâches au sein d'une même tâche ou de rechercher les tâches dans plusieurs files d'attente	Lecture	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchWorkers	Autorise la recherche de travailleurs dans plusieurs flottes	Lecture			identitystore:ListGroupMembershipsForMember
StartSessionsStatisticsAggregation	Autorise l'accès à toutes les statistiques collectées pour les sessions	Lecture	fleet		identitystore:ListGroupMembershipsForMember
			queue		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter ou de remplacer une ou plusieurs balises pour la ressource Deadline Cloud spécifiée	Identification	budget		
			farm		
			fleet		
			job		
			license-endpoint		
			monitor		
			queue		
			worker		
				aws:RequestTag/${TagKey} aws:TagKeys deadline:CalledAction	
UntagResource	Accorde l'autorisation de dissocier un ou plusieurs tags de la ressource Deadline Cloud spécifiée	Identification	budget		
			farm		
			fleet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			job		
			license-endpoint		
			monitor		
			queue		
			worker		
				aws:TagKeys	
UpdateBudget	Autorise la mise à jour d'un budget	Écrire	budget*		identitystore:ListGroupMembershipsForMember
UpdateFarm	Autorise la mise à jour d'une ferme	Écrire	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFleet	Autorise la mise à jour d'une flotte	Écrire	fleet*		ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway
UpdateJob	Accorde l'autorisation de mettre à jour une tâche.	Écrire	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateLimit	Autorise la mise à jour d'une limite pour une ferme	Écrire	farm*		identitystore:ListGroupMembershipsForMember
UpdateMonitor	Accorde l'autorisation de mettre à jour un moniteur	Écrire	monitor*		iam:PassRole sso:PutApplicationGrant sso:UpdateApplication
UpdateQueue	Autorise la mise à jour d'une file d'attente	Écrire	queue*		iam:PassRole identitystore:ListGroupMembershipsForMember
UpdateQueueEnvironment	Autorise la mise à jour d'un environnement de file d'attente	Écrire	queue*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateQueueFleetAssociation	Autorise la mise à jour d'une association de flottes de files d'attente	Écrire	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateQueueLimitAssociation	Autorise la mise à jour d'une association de limite de file d'attente	Écrire	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateSession	Accorde l'autorisation de mettre à jour une session pour une tâche	Écrire	job*		identitystore:ListGroupMembershipsForMember
UpdateStep	Accorde l'autorisation de mettre à jour une étape pour une tâche	Écrire	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateStorageProfile	Autorise la mise à jour d'un profil de stockage pour une ferme	Écrire	farm*		identitystore:ListGroupMembershipsForMember
UpdateTask	Accorde l'autorisation de mettre à jour une tâche	Écrire	job*		identitystore:ListGroupMembershipsForMember
UpdateWorker	Accorde l'autorisation de mettre à jour un employé	Écrire	worker*		logs:CreateLogStream
UpdateWorkerSchedule	Accorde l'autorisation de mettre à jour le planning d'un collaborateur	Écrire	worker*		logs:CreateLogStream

Types de ressources définis par AWS Deadline Cloud

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
budget	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/budget/${BudgetId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels
farm	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels
fleet	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels
job	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}/job/${JobId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:JobMembershipLevels deadline:QueueMembershipLevels
license-endpoint	arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
monitor	`arn:${Partition}:deadline:${Region}:${Account}:monitor/${MonitorId}`	aws:ResourceTag/${TagKey}
queue	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:QueueMembershipLevels
worker	`arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}/worker/${WorkerId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels

Clés de condition pour AWS Deadline Cloud

AWS Deadline Cloud définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
deadline:AssociatedMembershipLevel	Filtre l'accès en fonction du niveau d'adhésion associé au principal fourni dans la demande	String
deadline:CalledAction	Filtre l'accès en fonction de l'action autorisée dans la demande	String
deadline:FarmMembershipLevels	Filtre l'accès par niveau d'adhésion à la ferme	ArrayOfString
deadline:FleetMembershipLevels	Filtre l'accès par niveau d'adhésion sur la flotte	ArrayOfString
deadline:JobMembershipLevels	Filtre l'accès par niveau d'adhésion sur le lieu de travail	ArrayOfString
deadline:MembershipLevel	Filtre l'accès en fonction du niveau d'adhésion transmis dans la demande	String
deadline:PrincipalId	Filtre l'accès en fonction de l'identifiant principal fourni dans la demande	String
deadline:QueueMembershipLevels	Filtre l'accès par niveau d'adhésion dans la file d'attente	ArrayOfString

Clés de condition	Description	Type
deadline: RequesterPrincipalId	Filtre l'accès par l'utilisateur qui appelle l'API Deadline Cloud	String

Actions, ressources et clés de condition pour Amazon Detective

Amazon Detective (préfixe de service : `detective`) fournit les ressources, actions et clés de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Detective
- Types de ressources définis par Amazon Detective
- Clés de condition pour Amazon Detective

Actions définies par Amazon Detective

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptInvitation	Accorde l'autorisation d'accepter une invitation à devenir membre d'un graphique de comportement	Écrire	Graph*		
BatchGetGraphMemberDatasources	Accorde l'autorisation de récupérer l'historique du package de source de données pour les comptes membres spécifiés dans un graphique de comportement géré par ce compte	Lecture	Graph*		
BatchGetMembershipDatasources	Accorde l'autorisation de récupérer l'historique du package de source de données du compte de l'appelant pour les graphiques spécifiés	Lecture			
CreateGraph	Accorde l'autorisation de créer un graphique de comportement et de commencer à agréger les informations de sécurité	Écriture		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	detective:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMembers	Accorde l'autorisation de demander l'adhésion d'un ou de plusieurs comptes dans un graphique de comportement géré par ce compte	Écriture	Graph*		
DeleteGraph	Accorde l'autorisation de supprimer un graphique de comportement et d'arrêter l'agrégation des informations de sécurité	Écriture	Graph*		
DeleteMembers	Accorde l'autorisation de supprimer des comptes membres d'un graphique de comportement géré par ce compte	Écrire	Graph*		
DescribeOrganizationConfiguration	Accorde l'autorisation de consulter la configuration actuelle liée à l'intégration d'Amazon Detective avec AWS Organizations	Lecture	Graph*		organizations:DescribeOrganization
DisableOrganizationAdminAccount	Accorde l'autorisation de supprimer le compte administrateur délégué Amazon Detective pour une organisation	Écrire			organizations:DescribeOrganization

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateMembership	Accorde l'autorisation de supprimer l'association de ce compte avec un graphique de comportement	Écrire	Graph*		
EnableOrganizationAdminAccount	Accorde l'autorisation de désigner le compte administrateur délégué Amazon Detective pour une organisation	Écrire			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
GetFreeTrialEligibility [autorisation uniquement]	Accorde l'autorisation de récupérer l'éligibilité d'un graphique de comportement pour une période d'essai gratuite	Lecture	Graph*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGraphIngestState [autorisation uniquement]	Accorde l'autorisation de récupérer l'état d'ingestion de données d'un graphique de comportement	Lecture	Graph*		
GetInvestigation	Octroie l'autorisation d'obtenir le statut et les métadonnées d'une enquête.	Lecture	Graph*		
GetMembers	Accorde l'autorisation de récupérer des détails sur les membres spécifiés d'un graphique de comportement	Lecture	Graph*		
GetPricingInformation [autorisation uniquement]	Accorde l'autorisation de récupérer des informations sur les tarifs d'Amazon Detective	Lecture			
GetUsageInformation [autorisation uniquement]	Accorde l'autorisation de répertorier les informations d'utilisation d'un graphique de comportement	Lecture	Graph*		
InvokeAssistant [autorisation uniquement]	Octroie l'autorisation d'invoquer l'assistant de Detective.	Lecture	Graph*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDatasourcePackages	Accorde l'autorisation de répertorier les états d'ingestion et les horodatages du package de source de données d'un graphique pour les changements d'état les plus récents dans un graphique de comportement géré par ce compte	List	Graph*		
ListGraphs	Accorde l'autorisation de répertorier les graphiques de comportement gérés par ce compte	List			
ListHighDegreeEntities [autorisation uniquement]	Accorde l'autorisation de récupérer des entités à volume élevé dont les relations ne peuvent pas être stockées par Detective	List	Graph*		
ListIndicators	Octroie l'autorisation de répertorier les indicateurs d'une enquête.	List	Graph*		
ListInvestigations	Octroie l'autorisation de répertorier les investigations d'un graphique comportemental.	List	Graph*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListInvitations	Accorde l'autorisation de récupérer des détails sur les graphiques de comportement auxquels ce compte a été invité à se joindre	Liste			
ListMembers	Accorde l'autorisation de récupérer des détails sur tous les membres d'un graphique de comportement	List	Graph*		
ListOrganizationAdminAccount	Accorde l'autorisation de consulter le compte administrateur délégué Amazon Detective actuel pour une organisation	List			organizations:DescribeOrganization
ListTagsForResource	Accorde l'autorisation de répertorier les valeurs de balise affectées à un graphique de comportement.	List	Graph*		
				aws:ResourceTag/${TagKey}	
RejectInvitation	Accorde l'autorisation de rejeter une invitation à devenir membre d'un graphique de comportement	Écriture	Graph*		
SearchGraph [autorisation uniquement]	Accorde l'autorisation de rechercher les données stockées dans un graphique de comportement	Lecture	Graph*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartInvestigation	Octroie l'autorisation de lancer des enquêtes.	Écrire	Graph*		
StartMonitoringMember	Accorde l'autorisation de démarrer l'intégration de données pour un compte membre dont l'état indique ACCEPTED_BUT_DISABLED	Écrire	Graph*		
TagResource	Accorde l'autorisation d'affecter des valeurs de balise à un graphique de comportement.	Balisage	Graph*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des valeurs de balise d'un graphique de comportement.	Identification	Graph*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDatasourcePackages	Accorde l'autorisation d'activer ou de désactiver le ou les packages de source de données dans un graphique de comportement géré par ce compte	Écrire	Graph*		
UpdateInvestigationState	Octroie l'autorisation de mettre à jour le statut et les métadonnées d'une enquête.	Écrire	Graph*		
UpdateOrganizationConfiguration	Accorde l'autorisation de mettre à jour la configuration actuelle liée à l'intégration d'Amazon Detective avec AWS Organizations	Écrire	Graph*		organizations:DescribeOrganization

Types de ressources définis par Amazon Detective

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Graph	`arn:${Partition}:detective:${Region}:${Account}:graph:${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Detective

Amazon Detective définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en spécifiant les étiquettes transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en spécifiant les étiquettes associées à la ressource	String
aws:TagKeys	Filtre l'accès en spécifiant les clés d'étiquettes transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Device Farm

AWS Device Farm (préfixe de service :`devicefarm`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Device Farm
- Types de ressources définis par AWS Device Farm
- Clés de condition pour AWS Device Farm

Actions définies par AWS Device Farm

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDevicePool	Accorde l'autorisation de créer un groupe d'appareils au sein d'un projet	Écriture	project*		
CreateInstanceProfile	Accorde l'autorisation de créer un profil d'instance d'appareil	Écriture			
CreateNetworkProfile	Accorde l'autorisation de créer un profil réseau au sein d'un projet	Écriture	project*		
CreateProject	Accorde l'autorisation de créer un projet pour des tests mobiles	Écrire			ec2:CreateNetworkInterface

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateRemoteAccessSession	Accorde l'autorisation de démarrer une session d'accès à distance sur une instance d'appareil	Écriture	device*		
			project*		
			deviceinstance		
			upload		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTestGridProject	Accorde l'autorisation de créer un projet pour des tests de bureau	Écriture			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateTestGridUrl	Accorde l'autorisation de générer une nouvelle URL pré-signée utilisée pour accéder à notre service de grille de test	Écriture	testgrid-project*		
CreateUpload	Accorde l'autorisation de charger un nouveau fichier ou une nouvelle application dans un projet	Écriture	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateVPCEConfiguration	Accorde l'autorisation de créer une configuration de point de terminaison Amazon Virtual Private Cloud (VPC)	Écriture			
DeleteDevicePool	Accorde l'autorisation de supprimer un groupe d'appareils généré par l'utilisateur	Écriture	devicepool*		
DeleteInstanceProfile	Accorde l'autorisation de supprimer un profil d'instance généré par l'utilisateur	Écriture	instanceprofile*		
DeleteNetworkProfile	Accorde l'autorisation de supprimer un profil réseau généré par l'utilisateur	Écriture	networkprofile*		
DeleteProject	Accorde l'autorisation de supprimer un projet de test mobile	Écriture	project*		
DeleteRemoteAccessSession	Accorde l'autorisation de supprimer une session d'accès à distance terminée et ses résultats	Écriture	session*		
DeleteRun	Accorde l'autorisation de supprimer une exécution	Écriture	run*		
DeleteTestGridProject	Accorde l'autorisation de supprimer un projet de test de bureau	Écriture	testgrid-project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteUpload	Accorde l'autorisation de supprimer un fichier chargé par l'utilisateur	Écriture	upload*		
DeleteVPCEConfiguration	Accorde l'autorisation de supprimer une configuration de point de terminaison Amazon Virtual Private Cloud (VPC)	Écrire	vpceconfiguration*		
GetAccountSettings	Accorde l'autorisation de récupérer le nombre d'appareils iOS and/or non mesurés et Android achetés par le compte	Lecture			
GetDevice	Accorde l'autorisation de récupérer les informations d'un type d'appareil unique	Lecture	device*		
GetDeviceInstance	Accorde l'autorisation de récupérer les informations d'une instance d'appareil	Lecture	deviceinstance*		
GetDevicePool	Accorde l'autorisation de récupérer les informations d'un groupe d'appareils	Lecture	devicepool*		
GetDevicePoolCompatibility	Accorde l'autorisation de récupérer des informations sur la compatibilité d'une and/or application de test avec un pool d'appareils	Lecture	devicepool* upload		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInstanceProfile	Accorde l'autorisation de récupérer les informations d'un profil d'instance	Lecture	instanceprofile*		
GetJob	Accorde l'autorisation de récupérer les informations d'une tâche	Lecture	job*		
GetNetworkProfile	Accorde l'autorisation de récupérer les informations d'un profil réseau	Lecture	networkprofile*		
GetOfferingStatus	Accorde l'autorisation de récupérer le statut actuel et futur de toutes les offres achetées par un Compte AWS	Lecture			
GetProject	Accorde l'autorisation de récupérer des informations sur un projet de test mobile	Lecture	project*		
GetRemoteAccessSession	Accorde l'autorisation de supprimer le lien vers une session d'accès à distance en cours d'exécution	Lecture	session*		
GetRun	Accorde l'autorisation de récupérer les informations d'une exécution	Lecture	run*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSuite	Accorde l'autorisation de récupérer les informations d'une suite de test	Lecture	suite*		
GetTest	Accorde l'autorisation de récupérer les informations d'un cas de test	Lecture	test*		
GetTestGridProject	Accorde l'autorisation de récupérer des informations sur un projet de test de bureau	Lecture	testgrid-project*		
GetTestGridSession	Accorde l'autorisation de récupérer les informations d'une session de grille de test	Lecture	testgrid-project		
			testgrid-session		
GetUpload	Accorde l'autorisation de récupérer les informations d'un fichier chargé	Lecture	upload*		
GetVPCEConfiguration	Accorde l'autorisation de récupérer les informations d'une configuration de point de terminaison Amazon Virtual Private Cloud (VPC)	Lecture	vpceconfiguration*		
InstallToRemoteAccessSession	Accorde l'autorisation d'installer une application sur un appareil dans une session d'accès à distance	Écriture	session*		
			upload*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListArtifacts	Accorde l'autorisation de répertorier les artefacts d'un projet	Liste	job		
			run		
			suite		
			test		
ListDeviceInstances	Accorde l'autorisation de répertorier les informations des instances d'appareil	Liste			
ListDevicePools	Accorde l'autorisation de répertorier les informations des groupes d'appareils	Liste	project*		
ListDevices	Accorde l'autorisation de répertorier les informations de types d'appareils uniques	Liste			
ListInstanceProfiles	Accorde l'autorisation de répertorier les informations des profils d'instance d'appareil	Liste			
ListJobs	Accorde l'autorisation de répertorier les informations des tâches au sein d'une exécution	Liste	run*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNetworkProfiles	Accorde l'autorisation de répertorier les informations des profils réseau au sein d'un projet	Liste	project*		
ListOfferingPromotions	Accorde l'autorisation de répertorier les promotions de l'offre	List			
ListOfferingTransactions	Permet de répertorier tous les achats, renouvellements et transactions de renouvellement du système historiques pour un Compte AWS	List			
ListOfferings	Accorde l'autorisation de répertorier les produits ou les offres que l'utilisateur peut gérer via l'API	List			
ListProjects	Accorde l'autorisation de répertorier les informations des projets de test mobile pour un Compte AWS	List			
ListRemoteAccessSessions	Accorde l'autorisation de répertorier les informations des sessions d'accès à distance en cours d'exécution	Liste	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRuns	Accorde l'autorisation de répertorier les informations des exécutions au sein d'un projet	Liste	project*		
ListSamples	Accorde l'autorisation de répertorier les informations des exemples au sein d'un projet	Liste	job*		
ListSuites	Accorde l'autorisation de répertorier les informations des suites de test au sein d'une tâche	Liste	job*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	List	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
ListTestGridProjects	Accorde l'autorisation de répertorier les informations des projets de test de bureau pour un Compte AWS	List			
ListTestGridSessionActions	Accorde l'autorisation de répertorier les actions de session effectuées au cours d'une session de grille de test	Liste	testgrid-session*		
ListTestGridSessionArtifacts	Accorde l'autorisation de répertorier les artefacts générés par une session de grille de test	Liste	testgrid-session*		
ListTestGridSessions	Accorde l'autorisation de répertorier les sessions dans un projet de grille de test	Liste	testgrid-project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTests	Accorde l'autorisation de répertorier les informations des tests au sein d'une suite de tests	Liste	suite*		
ListUniqueProblems	Accorde l'autorisation de répertorier les informations relatives aux problèmes uniques au sein d'une exécution	Liste	run*		
ListUploads	Accorde l'autorisation de répertorier les informations des chargements au sein d'un projet	Liste	project*		
ListVPCEConfigurations	Accorde l'autorisation de répertorier les informations des configurations de point de terminaison Amazon Virtual Private Cloud (VPC)	List			
PurchaseOffering	Accorde l'autorisation d'acheter des offres pour un Compte AWS	Écrire			
RenewOffering	Accorde l'autorisation de définir la quantité d'appareils à renouveler pour une offre	Écriture			
ScheduleRun	Accorde l'autorisation de planifier une exécution	Écriture	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			devicepool		
			upload		
	SCÉNARIO : Device Pool as filter		devicepool* project* upload		
	SCÉNARIO : Device Selection Configuration as filter		project* upload		
StopJob	Accorde l'autorisation de mettre fin à une tâche en cours d'exécution	Écriture	job*		
StopRemoteAccessSession	Accorde l'autorisation de mettre fin à une session d'accès à distance en cours d'exécution	Écriture	session*		
StopRun	Accorde l'autorisation de mettre fin à une série de tests en cours d'exécution	Écriture	run*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	device		
			deviceinstance		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Balisage	device		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:TagKeys	
UpdateDeviceInstance	Accorde l'autorisation de modifier une instance d'appareil existante	Écriture	deviceinstance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			instanceprofile		
UpdateDevicePool	Accorde l'autorisation de modifier un groupe d'appareils existant	Écriture	devicepool*		
UpdateInstanceProfile	Accorde l'autorisation de modifier un profil d'instance existant	Écriture	instanceprofile*		
UpdateNetworkProfile	Accorde l'autorisation de modifier un profil réseau existant	Écriture	networkprofile*		
UpdateProject	Accorde l'autorisation de modifier un projet de test mobile existant	Écriture	project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTestGridProject	Accorde l'autorisation de modifier un projet de test de bureau existant	Écriture	testgrid-project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
UpdateUpload	Accorde l'autorisation de modifier un chargement existant	Écriture	upload*		
UpdateVPCEConfiguration	Accorde l'autorisation de modifier une configuration de point de terminaison Amazon Virtual Private Cloud (VPC) existante	Écrire	vpceconfiguration*		

Types de ressources définis par AWS Device Farm

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
project	`arn:${Partition}:devicefarm:${Region}:${Account}:project:${ResourceId}`	aws:ResourceTag/${TagKey}
run	`arn:${Partition}:devicefarm:${Region}:${Account}:run:${ResourceId}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:devicefarm:${Region}:${Account}:job:${ResourceId}`	
suite	`arn:${Partition}:devicefarm:${Region}:${Account}:suite:${ResourceId}`	
test	`arn:${Partition}:devicefarm:${Region}:${Account}:test:${ResourceId}`	
upload	`arn:${Partition}:devicefarm:${Region}:${Account}:upload:${ResourceId}`	
artifact	`arn:${Partition}:devicefarm:${Region}:${Account}:artifact:${ResourceId}`	
sample	`arn:${Partition}:devicefarm:${Region}:${Account}:sample:${ResourceId}`	
networkprofile	`arn:${Partition}:devicefarm:${Region}:${Account}:networkprofile:${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
deviceinstance	arn:${Partition}:devicefarm:${Region}::deviceinstance:${ResourceId}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:devicefarm:${Region}:${Account}:session:${ResourceId}	aws:ResourceTag/${TagKey}
devicepool	arn:${Partition}:devicefarm:${Region}:${Account}:devicepool:${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:devicefarm:${Region}::device:${ResourceId}	aws:ResourceTag/${TagKey}
instanceprofile	arn:${Partition}:devicefarm:${Region}:${Account}:instanceprofile:${ResourceId}	aws:ResourceTag/${TagKey}
vpceconfiguration	arn:${Partition}:devicefarm:${Region}:${Account}:vpceconfiguration:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-project	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-project:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-session	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-session:${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Device Farm

AWS Device Farm définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de l'ensemble des valeurs autorisées pour chacune des balises.	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur de balise associé à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour le service AWS DevOps d'agent

AWS DevOps Agent Service (préfixe de service :`aidevops`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS DevOps Agent Service
- Types de ressources définis par AWS DevOps Agent Service
- Clés de condition pour AWS DevOps Agent Service

Actions définies par AWS DevOps Agent Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation d'autoriser les journaux vendus	Gestion des autorisations			
AssociateService	Accorde l'autorisation d'associer un service	Écrire	agentspace*		
			associations*		
CreateAgentSpace	Accorde l'autorisation de créer un espace agent	Écrire	agentspace*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateBacklogTask	Accorde l'autorisation de créer une nouvelle tâche de backlog	Écrire	agentspace*		
CreateChat	Accorde l'autorisation de créer un chat	Écrire	agentspace*		
CreateKnowledgeItem	Accorde l'autorisation de créer un nouvel élément de connaissance	Écrire	agentspace*		
CreateOneTimeLoginSession	Accorde l'autorisation de générer une session unique sécurisée pour initier la connexion à l'application hors console	Écrire	agentspace*		
DeleteAgentSpace	Accorde l'autorisation de supprimer l'espace agent	Écrire	agentspace*		
				aws:ResourceTag/${TagKey}	
DeleteKnowledgeItem	Accorde l'autorisation de supprimer un élément de connaissance	Écrire	agentspace*		
DeregisterService	Accorde l'autorisation de désenregistrer un service	Écrire	service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DescribeSupportLevel	Accorde l'autorisation de décrire un chat dans le cadre d'un dossier	Écrire	agentspace*		
DisableOperatorApp	Accorde l'autorisation de désactiver l'accès de l'application Operator au AgentSpace	Écrire	agentspace*		
DisassociateService	Accorde l'autorisation de dissocier le service	Écrire	agentspace*		
			associations*		
DiscoverTopology	Autorise la découverte d'informations topologiques	Écrire	agentspace*		
EnableOperatorApp	Accorde l'autorisation d'autoriser l'application Operator à accéder aux données AgentSpace	Écrire	agentspace*		
EndChatForCase	Accorde l'autorisation de mettre fin à une discussion pour un dossier	Écrire	agentspace*		
GetAccountUsage	Accorde l'autorisation de récupérer les informations d'utilisation du compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAgentSpace	Accorde l'autorisation d'obtenir de l'espace agent	Lecture	agentspace*		
				aws:ResourceTag/${TagKey}	
GetAssociation	Donne l'autorisation de créer une association	Lecture	agentspace*		
			associations*		
GetBacklogTask	Accorde l'autorisation d'obtenir une tâche en attente	Lecture	agentspace*		
GetKnowledgeItem	Accorde l'autorisation d'obtenir un élément de connaissance	Lecture	agentspace*		
GetOperatorApp	Accorde l'autorisation d'obtenir la configuration d'authentification de l'opérateur pour tout flux d'authentification activé	Lecture	agentspace*		
GetRecommendation	Accorde l'autorisation d'obtenir une recommandation	Lecture	agentspace*		
GetService	Donne l'autorisation d'obtenir des services	Lecture	service*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InitiateChatForCase	Accorde l'autorisation d'initier une discussion pour un dossier	Écrire	agentspace*		
ListAgentSpaces	Accorde l'autorisation de répertorier l'espace agent	List			
ListAssociations	Accorde l'autorisation de répertorier les associations	List	agentspace*		
ListBacklogTasks	Accorde l'autorisation de répertorier les tâches en attente	List	agentspace*		
ListChats	Accorde l'autorisation de répertorier les chats	List	agentspace*		
ListExecutions	Permet de répertorier les exécutions	List	agentspace*		
ListGoals	Accorde l'autorisation de répertorier les objectifs	List	agentspace*		
ListJournalRecords	Donne l'autorisation de répertorier les documents du journal	List	agentspace*		
ListKnowledgeItemVersions	Accorde l'autorisation de répertorier les versions des éléments de connaissances	List	agentspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListKnowledgeItems	Accorde l'autorisation de répertorier les éléments de connaissances	List	agentspace*		
ListPendingMessages	Accorde l'autorisation de répertorier les messages en attente	List	agentspace*		
ListRecommendations	Accorde l'autorisation de répertorier les recommandations	List	agentspace*		
ListServices	Accorde l'autorisation de répertorier les services	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	agentspace	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	
ListWebhooks	Accorde l'autorisation de répertorier les webhooks pour l'association	List	agentspace*		
			associations*		
RegisterService	Accorde l'autorisation d'enregistrer un service spécifique	Écrire	service*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchServiceAccessibleResource	Accorde l'autorisation de rechercher des ressources accessibles à un service enregistré	Lecture			
SendMessage	Accorde l'autorisation d'envoyer des messages de chat	Écrire	agentspace*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	agentspace	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
			service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	agentspace	aws:ResourceTag/${TagKey} aws:TagKeys	
			service	aws:ResourceTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgentSpace	Autorise la mise à jour de l'espace agent	Écrire	agentspace*		
				aws:ResourceTag/${TagKey}	
UpdateAssociation	Autorise la mise à jour de l'association	Écrire	agentspace*		
			associations*		
UpdateBacklogTask	Accorde l'autorisation de mettre à jour une tâche	Écrire	agentspace*		
UpdateGoal	Autorise la mise à jour d'un objectif	Écrire	agentspace*		
UpdateKnowledgeItem	Accorde l'autorisation de mettre à jour un élément de connaissance	Écrire	agentspace*		
UpdateOperatorAppIdpConfig	Accorde l'autorisation de mettre à jour la configuration du fournisseur d'identité externe pour l'application Operator	Écrire	agentspace*		
UpdateRecommendation	Autorise la mise à jour d'une recommandation	Écrire	agentspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ValidateAwsAssociations	Accorde l'autorisation de valider l'association AWS	Écrire	agentspace*		

Types de ressources définis par AWS DevOps Agent Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
agentspace	`arn:${Partition}:aidevops:${Region}:${Account}:agentspace/${AgentSpaceId}`	aws:ResourceTag/${TagKey}
associations	`arn:${Partition}:aidevops:${Region}:${Account}:agentspace/${AgentSpaceId}/associations/${AssociationId}`	
service	`arn:${Partition}:aidevops:${Region}:${Account}:service/${ServiceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS DevOps Agent Service

AWS DevOps Agent Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon DevOps Guru

Amazon DevOps Guru (préfixe de service :`devops-guru`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon DevOps Guru

- Types de ressources définis par Amazon DevOps Guru
- Clés de condition pour Amazon DevOps Guru

Actions définies par Amazon DevOps Guru

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddNotificationChannel	Accorde l'autorisation d'ajouter un canal de notification à DevOps Guru	Écrire	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
DeleteInsight	Accorde l'autorisation de supprimer des informations spécifiées dans votre compte	Écrire			
DescribeAccountHealth	Permet de consulter l'état des opérations dans votre Compte AWS	Lecture			
DescribeAccountOverview	Permet de consulter l'état des opérations dans un intervalle de temps donné dans votre Compte AWS	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAnomaly	Accorde l'autorisation de répertorier les informations d'une anomalie spécifiée	Lecture			
DescribeEventSourcesConfig	Accorde l'autorisation de récupérer des informations sur les sources d'événements pour DevOps Guru	Lecture			
DescribeFeedback	Accorde l'autorisation d'afficher les commentaires relatifs à une information spécifiée	Lecture			
DescribeInsight	Accorde l'autorisation de répertorier les informations d'une information spécifiée.	Lecture			
DescribeOrganizationHealth	Accorde l'autorisation d'afficher l'état des opérations dans votre organisation	Lecture			
DescribeOrganizationOverview	Accorde l'autorisation d'afficher l'état des opérations dans un créneau horaire dans votre organisation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeOrganizationResourceCollectionHealth	Accorde l'autorisation de consulter l'état des opérations pour chaque AWS CloudFormation pile, AWS services ou comptes spécifiés dans DevOps Guru au sein de votre organisation	Lecture			
DescribeResourceCollectionHealth	Permet de consulter l'état des opérations pour chaque AWS CloudFormation pile spécifiée dans DevOps Guru	Lecture			
DescribeServiceIntegration	Accorde l'autorisation de consulter le statut d'intégration des services pouvant être intégrés à DevOps Guru	Lecture			
GetCostEstimation	Accorde l'autorisation de répertorier les estimations de coûts des ressources du service	Lecture			
GetResourceCollection	Accorde l'autorisation de répertorier AWS CloudFormation les piles que DevOps Guru est configuré pour utiliser	Lecture			
ListAnomaliesForInsight	Accorde l'autorisation de répertorier les anomalies d'une information donnée dans votre compte.	List		devops-guru:ServiceNames	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAnomalousLogGroups	Accorde l'autorisation de répertorier les anomalies de journal d'une information donnée dans votre compte	List			
ListEvents	Accorde l'autorisation de répertorier les événements liés aux ressources évalués par DevOps Guru	List			
ListInsights	Accorde l'autorisation de répertorier les informations de votre compte.	List			
ListMonitoredResources	Accorde l'autorisation de répertorier les ressources surveillées par DevOps Guru sur votre compte	List			
ListNotificationChannels	Permet de répertorier les canaux de notification configurés pour DevOps Guru dans votre compte	List			
ListOrganizationInsights	Accorde l'autorisation de répertorier les informations de votre organisation	List			
ListRecommendations	Accorde l'autorisation de répertorier les recommandations d'une information spécifiée.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutFeedback	Accorde l'autorisation de soumettre un commentaire à DevOps Guru	Écrire			
RemoveNotificationChannel	Accorde l'autorisation de supprimer un canal de notification de DevOps Guru	Écrire	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
SearchInsights	Accorde l'autorisation de rechercher des informations dans votre compte.	List		devops-guru:ServiceNames	
SearchOrganizationInsights	Accorde l'autorisation de rechercher des informations dans votre organisation	List			
StartCostEstimation	Accorde l'autorisation d'entamer la création d'une estimation du coût mensuel	Lecture			
UpdateEventSourcesConfig	Autorise la mise à jour d'une source d'événement pour DevOps Guru	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateResourceCollection	Permet de mettre à jour la liste des AWS CloudFormation piles utilisées pour spécifier les AWS ressources de votre compte analysées par Guru DevOps	Écrire			
UpdateServiceIntegration	Accorde l'autorisation d'activer ou de désactiver un service qui s'intègre à DevOps Guru	Écrire			

Types de ressources définis par Amazon DevOps Guru

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	

Clés de condition pour Amazon DevOps Guru

Amazon DevOps Guru définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
devops-guru:ServiceNames	Filtre l'accès par API pour restreindre l'accès à des noms AWS de service donnés	ArrayOfString

Actions, ressources et clés de condition pour les outils AWS de diagnostic

AWS Les outils de diagnostic (préfixe de service :`ts`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les outils AWS de diagnostic
- Types de ressources définis par les outils AWS de diagnostic
- Clés de condition pour les outils AWS de diagnostic

Actions définies par les outils AWS de diagnostic

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExecution	Accorde l'autorisation d'obtenir des détails sur une exécution spécifique dans les outils AWS de diagnostic	Lecture	execution*		
GetExecutionOutput	Accorde l'autorisation d'obtenir des détails sur une sortie d'exécution spécifique dans les outils AWS de diagnostic	Lecture	execution*		
GetTool	Accorde l'autorisation d'obtenir des informations sur un outil spécifique dans les outils AWS de diagnostic	Lecture	tool*		
ListExecutions	Accorde l'autorisation de répertorier toutes les exécutions disponibles dans les outils AWS de diagnostic	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource d'outils AWS de diagnostic	Lecture	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTools	Accorde l'autorisation de répertorier tous les outils	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	disponibles dans les outils AWS de diagnostic				
StartExecution	Accorde l'autorisation de démarrer un flux de travail d'exécution d'un outil spécifique dans les outils AWS de diagnostic	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
TagResource	Accorde l'autorisation de baliser une ressource d'outils de AWS diagnostic	Identification	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource d'outils AWS de diagnostic	Identification	execution*		
				aws:TagKeys	

Types de ressources définis par les outils AWS de diagnostic

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
execution	`arn:${Partition}:ts::${Account}:execution/${UserId}/${ToolId}/${ExecutionId}`	aws:ResourceTag/${TagKey}
tool	`arn:${Partition}:ts::aws:tool/${ToolId}`	

Clés de condition pour les outils AWS de diagnostic

AWS Les outils de diagnostic définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Direct Connect

AWS Direct Connect (préfixe de service :`directconnect`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Direct Connect
- Types de ressources définis par AWS Direct Connect
- Clés de condition pour AWS Direct Connect

Actions définies par AWS Direct Connect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptDirectConnectGatewayAssociationProposal	Accorde l'autorisation d'accepter une demande de proposition visant à attacher une passerelle réseau privé virtuel à une passerelle Direct Connect	Écrire	dx-gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllocateConnectionOnInterconnect	Accorde l'autorisation de créer une connexion hébergée sur une interconnexion	Écrire	dxcon*		
AllocateHostedConnection	Autorise la création d'une nouvelle connexion hébergée entre le réseau d'un partenaire AWS Direct Connect et un emplacement AWS Direct Connect spécifique	Écrire	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePrivateVirtualInterface	Accorde l'autorisation d'allouer une interface virtuelle privée devant être détenue par un autre client	Écrire	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePublicVirtualInterface	Accorde l'autorisation d'allouer une interface virtuelle publique devant être détenue par un autre client	Écrire	dxcon		
			dxlag		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocateTransitVirtualInterface	Accorde l'autorisation d'allouer une interface virtuelle de transit devant être détenue par un autre client	Écrire	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateConnectionWithLag	Accorde l'autorisation d'associer une connexion à un LAG	Écrire	dxcon*		
			dxlag*		
AssociateHostedConnection	Accorde l'autorisation d'associer une connexion hébergée et ses interfaces virtuelles à un groupe d'agrégation de liaisons (LAG) ou une interconnexion	Écrire	dxcon*		
			dxcon		
			dxlag		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateMacSecKey	Permet d'associer une paire MAC Security (MACsec) Connection Key Name (CKN) / Connectivity Association Key (CAK) à une AWS connexion dédiée Direct Connect	Écrire	dxcon		
			dxlag		
AssociateVirtualInterface	Accorde l'autorisation d'associer une interface virtuelle à un groupe d'agrégation de liaisons (LAG) ou une connexion spécifié(e)	Écrire	dxvif*		
			dxcon		
			dxlag		
ConfirmConnection	Accorde l'autorisation de confirmer la création d'une connexion hébergée sur une interconnexion	Écrire	dxcon*		
ConfirmCustomerAgreement	Accorde l'autorisation de confirmer les conditions du contrat lors de la création de la connexion ou du groupe d'agrégation de liaisons (LAG)	Écrire			
ConfirmPrivateVirtualInterface	Accorde l'autorisation d'accepter la propriété d'une interface virtuelle privée créée par un autre client	Écrire	dxvif*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConfirmPublicVirtualInterface	Accorde l'autorisation d'accepter la propriété d'une interface virtuelle publique créée par un autre client	Écrire	dxvif*		
ConfirmTransitVirtualInterface	Accorde l'autorisation d'accepter la propriété d'une interface virtuelle de transit créée par un autre client	Écrire	dxvif*		
CreateBGPPeer	Accorde l'autorisation de créer un appairage BGP sur l'interface virtuelle spécifiée	Écrire	dxvif*		
CreateConnection	Accorde l'autorisation de créer une nouvelle connexion entre le réseau du client et un emplacement AWS Direct Connect spécifique	Écrire	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGateway	Accorde l'autorisation de créer une passerelle Direct Connect, qui est un objet intermédiaire permettant de connecter un ensemble d'interfaces virtuelles et de passerelles privées virtuelles	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDirectConnectGatewayAssociation	Accorde l'autorisation de créer une association entre une passerelle Direct Connect et une passerelle réseau privé virtuel	Écrire	dx-gateway*		
CreateDirectConnectGatewayAssociationProposal	Accorde l'autorisation de créer une proposition visant à associer la passerelle réseau privé virtuel spécifiée à la passerelle Direct Connect spécifiée	Écrire	dx-gateway*		
CreateInterconnect	Autorise la création d'une nouvelle interconnexion entre le réseau d'un partenaire AWS Direct Connect et un emplacement AWS Direct Connect spécifique	Écrire	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLag	Accorde l'autorisation de créer un groupe d'agrégation de liens (LAG) avec le nombre spécifié de connexions physiques groupées entre le réseau du client et un emplacement AWS Direct Connect spécifique	Écrire	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePrivateVirtualInterface	Accorde l'autorisation de créer une interface virtuelle privée	Écrire	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	Accorde l'autorisation de créer une interface virtuelle publique	Écrire	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	Accorde l'autorisation de créer une interface virtuelle de transit	Écrire	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBGPPeer	Accorde l'autorisation de supprimer l'appairage BGP spécifié sur l'interface virtuelle spécifiée avec l'adresse client et l'ASN spécifiés	Écrire	dxvif*		
DeleteConnection	Accorde l'autorisation de supprimer la connexion	Écrire	dxcon*		
DeleteDirectConnectGateway	Accorde l'autorisation de supprimer la passerelle Direct Connect spécifiée	Écrire	dx-gateway*		
DeleteDirectConnectGatewayAssociation	Accorde l'autorisation de supprimer l'association entre la passerelle Direct Connect spécifiée et la passerelle réseau privé virtuel	Écrire	dx-gateway*		
DeleteDirectConnectGatewayAssociationProposal	Accorde l'autorisation de supprimer la demande de proposition d'association entre la passerelle Direct Connect spécifiée et la passerelle réseau privé virtuel	Écrire			
DeleteInterconnect	Accorde l'autorisation de supprimer l'interconnexion spécifiée	Écrire	dxcon*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLag	Accorde l'autorisation de supprimer le groupe d'agrégation de liaisons (LAG) spécifié	Écrire	dxlag*		
DeleteVirtualInterface	Accorde l'autorisation de supprimer une interface virtuelle	Écrire	dxvif*		
DescribeConnectionLoa	Accorde l'autorisation de décrire la LOA-CFA pour une connexion	Lecture	dxcon*		
DescribeConnections	Accorde l'autorisation de décrire toutes les connexions dans cette région	Lecture	dxcon		
DescribeConnectionsOnInterconnect	Accorde l'autorisation de décrire une liste des connexions qui ont été allouées sur l'interconnexion donnée	Lecture	dxcon*		
DescribeCustomerMetadata	Accorde l'autorisation de consulter une liste des accords avec les clients, ainsi que leur statut signé et indique si le client est un NNIPartner, un NNIPartner V2 ou un non-partenaire	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDirectConnectGatewayAssociationProposals	Accorde l'autorisation de décrire une ou plusieurs propositions d'association pour la connexion entre une passerelle réseau privé virtuel et une passerelle Direct Connect	Lecture	dx-gateway		
DescribeDirectConnectGatewayAssociations	Accorde l'autorisation de décrire les associations entre vos passerelles Direct Connect et les passerelles réseau privé virtuel	Lecture	dx-gateway		
DescribeDirectConnectGatewayAttachments	Accorde l'autorisation de décrire les attachements entre vos passerelles Direct Connect et les interfaces virtuelles	Lecture	dx-gateway		
DescribeDirectConnectGateways	Accorde l'autorisation de décrire toutes vos passerelles Direct Connect ou la passerelle Direct Connect spécifiée uniquement	Lecture	dx-gateway		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeHostedConnections	Accorde l'autorisation de décrire les connexions hébergées qui ont été allouées sur l'interconnexion ou le groupe d'agrégation de liaisons (LAG) spécifié(e)	Lecture	dxcon		
			dxlag		
DescribeInterconnectLoa	Accorde l'autorisation de décrire la LOA-CFA pour une interconnexion	Lecture	dxcon*		
DescribeInterconnects	Octroie l'autorisation de décrire une liste d'interconnexions détenues par Compte AWS	Lecture	dxcon		
DescribeLags	Accorde l'autorisation de décrire tous vos groupes d'agrégation de liaisons (LAG) ou le LAG spécifié	Lecture	dxlag		
DescribeLoa	Accorde l'autorisation de décrire la LOA-CFA pour une connexion, une interconnexion ou un groupe d'agrégation de liaisons (LAG)	Lecture	dxcon		
			dxlag		
DescribeLocations	Accorde l'autorisation de décrire la liste des sites AWS Direct Connect dans la AWS région actuelle	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRouterConfiguration	Accorde l'autorisation de décrire les informations sur le routeur pour une interface virtuelle	Lecture	dxvif*		
DescribeTags	Accorde l'autorisation de décrire les balises associées aux ressources AWS Direct Connect spécifiées	Lecture	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
DescribeVirtualGateways	Accorde l'autorisation de décrire une liste de passerelles privées virtuelles détenues par le Compte AWS	Lecture			
DescribeVirtualInterfaces	Accorde l'autorisation de décrire toutes les interfaces virtuelles d'un Compte AWS	Lecture	dxcon		
			dxlag		
			dxvif		
DisassociateConnectionFromLag	Accorde l'autorisation de dissocier une connexion d'un groupe d'agrégation de liaisons (LAG)	Écrire	dxcon*		
			dxlag*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateMacSecKey	Accorde l'autorisation de supprimer l'association entre une clé de sécurité MAC Security (MACsec) et une connexion dédiée AWS Direct Connect	Écrire	dxcon		
			dxlag		
ListVirtualInterfaceTestHistory	Accorde l'autorisation de répertorier l'historique des tests de basculement de l'interface virtuelle	List	dxvif*		
StartBgpFailoverTest	Accorde l'autorisation de lancer le test de basculement de l'interface virtuelle qui vérifie que votre configuration répond à vos exigences en matière de résilience, en plaçant la session d'appairage BGP dans l'état DOWN. Vous pouvez ensuite envoyer du trafic pour vérifier qu'il n'y a pas de pannes	Écrire	dxvif*		
StopBgpFailoverTest	Accorde l'autorisation d'arrêter le test de basculement de l'interface virtuelle	Écrire	dxvif*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter les balises spécifiées à la ressource AWS Direct Connect spécifiée. Chaque ressource peut avoir un maximum de 50 balises	Identification	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises de la ressource AWS Direct Connect spécifiée	Identification	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConnection	Accorde l'autorisation de mettre à jour la configuration de la connexion dédiée AWS Direct Connect. Vous pouvez mettre à jour les paramètres suivants pour une connexion : le nom de la connexion ou le mode de cryptage MAC Security (MACsec) de la connexion	Écrire	dxcon*		
UpdateDirectConnectGateway	Accorde l'autorisation de mettre à jour le nom d'une passerelle Direct Connect	Écrire	dx-gateway*		
UpdateDirectConnectGatewayAssociation	Accorde l'autorisation de mettre à jour les attributs spécifiés de l'association de passerelle Direct Connect	Écrire			
UpdateLag	Accorde l'autorisation de mettre à jour les attributs du groupe d'agrégation de liaisons (LAG) spécifié	Écrire	dxlag*		
UpdateVirtualInterfaceAttributes	Accorde l'autorisation de mettre à jour les attributs spécifiés de l'interface virtuelle privée spécifiée	Écrire	dxvif*		

Types de ressources définis par AWS Direct Connect

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`	aws:ResourceTag/${TagKey}
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`	aws:ResourceTag/${TagKey}
dxvif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`	aws:ResourceTag/${TagKey}
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Direct Connect

AWS Direct Connect définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d’application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des actions basées sur la présence de paires clé-valeur de balise dans la requête	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des actions basées sur les paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des actions basées sur la présence de clés d'identification dans la requête	ArrayOfString

Actions, ressources et clés de condition pour AWS Directory Service

AWS Directory Service (préfixe de service :`ds`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Directory Service
- Types de ressources définis par AWS Directory Service
- Clés de condition pour AWS Directory Service

Actions définies par AWS Directory Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptSharedDirectory	Accorde l'autorisation d'accepter une demande de partage d'annuaire qui a été envoyée depuis le compte propriétaire du répertoire	Écrire	directory*		
AccessDSData [autorisation uniquement]	Accorde l'autorisation d'accéder aux données d'annuaire à l'aide de l'API Directory Service Data	Gestion des autorisations	directory*		
AddIpRoutes	Accorde l'autorisation d'ajouter un bloc d'adresse CIDR pour acheminer correctement le trafic vers et depuis votre annuaire Microsoft AD on Amazon Web Services	Écrire	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DescribeSecurityGroups
AddRegion	Accorde l'autorisation d'ajouter deux contrôleurs de domaine dans la région spécifiée pour le répertoire spécifié	Écrire	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecur

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
AddTagsToResource	Accorde l'autorisation d'ajouter ou d'écraser une ou plusieurs identifications pour le répertoire Amazon Directory Services spécifié	Identification	directory*		ec2:CreateTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
Authorize Application [autorisation uniquement]	Accorde l'autorisation d'autoriser une application pour votre AWS annuaire	Écrire	directory*		
CancelSchemaExtension	Accorde l'autorisation d'annuler une extension de schéma en cours pour un répertoire Microsoft AD	Écrire	directory*		
CheckAlias [autorisation uniquement]	Accorde l'autorisation de vérifier que l'alias est disponible pour être utilisé	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConnectDirectory	Accorde l'autorisation de créer un AD Connector pour se connecter à un répertoire sur site	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAlias	Accorde l'autorisation de créer un alias pour un annuaire et d'attribuer l'alias au répertoire	Écrire	directory*		
CreateComputer	Accorde l'autorisation de créer un compte d'ordinateur dans l'annuaire spécifié et de joindre l'ordinateur au répertoire	Écrire	directory*		
CreateConditionalForwarder	Accorde l'autorisation de créer un redirecteur conditionnel associé à votre répertoire AWS	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDirectory	Accorde l'autorisation de créer un répertoire Simple AD	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateHybridAD	Accorde l'autorisation de créer un annuaire AD géré hybride	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole iam:GetRole secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ssm:ListCommands ssm:SendCommand
CreateIdentityPoolDirectory [autorisation uniquement]	Accorde l'autorisation de créer un IdentityPool annuaire dans le AWS cloud	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogSubscription	Accorde l'autorisation de créer un abonnement pour transférer les journaux de sécurité du contrôleur de domaine Directory Service en temps réel vers le groupe de CloudWatch journaux spécifié dans votre Compte AWS	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMicrosoftAD	Accorde l'autorisation de créer un Microsoft AD dans le AWS cloud	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSnapshot	Autorise la création d'un instantané d'un annuaire Simple AD ou Microsoft AD dans le AWS cloud	Écrire	directory*		
CreateTrust	Accorde l'autorisation d'initier la création AWS d'une relation de confiance entre un Microsoft AD dans le AWS cloud et un domaine externe	Écrire	directory*		
DeleteADAssessment	Accorde l'autorisation de supprimer une évaluation d'annuaire	Écrire			
DeleteConditionalForwarder	Autorise la suppression d'un redirecteur conditionnel configuré pour votre annuaire AWS	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDirectory	Accorde l'autorisation de supprimer un AWS annuaire du Directory Service	Écrire	directory*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress
DeleteLogSubscription	Accorde l'autorisation de supprimer l'abonnement au journal spécifié	Écrire	directory*		
DeleteSnapshot	Accorde l'autorisation de supprimer un instantané d'un répertoire	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTrust	Accorde l'autorisation de supprimer une relation de confiance existante entre votre Microsoft AD dans le AWS cloud et un domaine externe	Écrire	directory*		
DeregisterCertificate	Accorde l'autorisation de supprimer du système le certificat qui a été enregistré pour une connexion LDAP sécurisée	Écrire	directory*		
DeregisterEventTopic	Accorde l'autorisation de supprimer le répertoire spécifié en tant qu'éditeur de la rubrique SNS spécifiée	Écrire	directory*		
DescribeADAssessment	Accorde l'autorisation de décrire une évaluation d'un annuaire	Lecture			
DescribeCAEnrollmentPolicy	Accorde l'autorisation de décrire le statut d'inscription à l'autorité de certification d'un répertoire spécifié	Lecture	directory*		
DescribeCertificate	Accorde l'autorisation d'afficher des informations sur le certificat enregistré pour une connexion LDAP sécurisée	Lecture	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeClientAuthenticationSettings	Accorde l'autorisation de récupérer des informations sur le type d'authentification client pour le répertoire spécifié, si le type est spécifié. Si aucun type n'est spécifié, des informations sur tous les types d'authentification client pris en charge pour le répertoire spécifié sont récupérées. Actuellement, seul SmartCard est pris en charge	Lecture	directory*		
DescribeConditionalForwarders	Accorde l'autorisation d'obtenir des informations sur les redirecteurs conditionnels pour ce compte	Lecture	directory*		
DescribeDirectories	Accorde l'autorisation d'obtenir des informations sur les annuaires qui appartiennent à ce compte	List			
DescribeDirectoryDataAccess	Accorde l'autorisation de décrire le statut de l'API Directory Service Data pour le répertoire spécifié	Lecture	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDomainControllers	Accorde l'autorisation d'obtenir des informations sur tous les contrôleurs de domaine dans votre répertoire	Lecture	directory*		
DescribeEventTopics	Accorde l'autorisation d'obtenir des informations sur les rubriques SNS qui reçoivent des messages d'état du répertoire spécifié	Lecture	directory*		
DescribeHybridADUpdate	Accorde l'autorisation de décrire les mises à jour d'un répertoire hybride spécifié	Lecture	directory*		
DescribeLDAPSSettings	Accorde l'autorisation de décrire l'état de la sécurité LDAP pour le répertoire spécifié	Lecture	directory*		
DescribeRegions	Accorde l'autorisation de fournir des informations sur les régions qui sont configurées pour la réplication multirégions	Lecture	directory*		
DescribeSettings	Accorde l'autorisation de récupérer des informations sur les paramètres configurables pour le répertoire spécifié	Lecture	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSharedDirectories	Accorde l'autorisation de renvoyer les annuaires partagés de votre compte	Lecture	directory*		
DescribeSnapshots	Accorde l'autorisation d'obtenir des informations sur les instantanés du répertoire qui appartiennent à ce compte	Lecture			
DescribeTrusts	Accorde l'autorisation d'obtenir des informations sur les relations d'approbation pour ce compte	Lecture			
DescribeUpdateDirectory	Accorde l'autorisation à décrire les mises à jour d'un répertoire pour un type de mise à jour particulier	Lecture	directory*		
DisableCAEnrollmentPolicy	Accorde l'autorisation de désactiver l'inscription au CA d'un répertoire spécifié	Écrire	directory*		
DisableClientAuthentication	Accorde l'autorisation de désactiver les méthodes alternatives d'authentification client pour l'annuaire spécifié	Écrire	directory*		
DisableDirectoryDataAccess	Accorde l'autorisation de désactiver l'API Directory Service Data pour le répertoire spécifié	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableLDAPS	Accorde l'autorisation de désactiver les appels sécurisés LDAP pour le répertoire spécifié	Écrire	directory*		
DisableRadius	Accorde l'autorisation de désactiver l'authentification multifacteur (MFA) avec le serveur RADIUS (Remote Authentication Dial In User Service) pour un répertoire AD Connector	Écrire	directory*		
DisableRoleAccess [autorisation uniquement]	Accorde l'autorisation de désactiver AWS Management Console l'accès pour l'identité dans votre AWS annuaire	Écrire	directory*		
DisableSso	Accorde l'autorisation de désactiver l'authentification unique pour un répertoire	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableCAEnrollmentPolicy	Accorde l'autorisation d'activer l'inscription en tant que CA d'un répertoire spécifié	Écrire	directory*		acm-pca:DescribeCertificateAuthority pca-connector-ad:GetConnector
EnableClientAuthentication	Accorde l'autorisation d'activer les méthodes alternatives d'authentification client pour le répertoire spécifié	Écrire	directory*		
EnableDirectoryDataAccess	Accorde l'autorisation d'activer l'API Directory Service Data pour le répertoire spécifié	Écrire	directory*		
EnableLDAPS	Accorde l'autorisation d'activer le commutateur pour le répertoire spécifique afin de toujours utiliser les appels sécurisés LDAP	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableRadius	Accorde l'autorisation d'activer l'authentification multifacteur (MFA) avec le serveur RADIUS (Remote Authentication Dial In User Service) pour un répertoire AD Connector	Écrire	directory*		
EnableRoleAccess [autorisation uniquement]	Accorde l'autorisation d'activer AWS Management Console l'accès pour l'identité dans votre AWS annuaire	Écrire	directory*		iam:PassRole
EnableSso	Accorde l'autorisation d'activer l'authentification unique pour un répertoire	Écrire	directory*		
GetAuthorizedApplicationDetails [autorisation uniquement]	Accorde l'autorisation de récupérer les détails des applications autorisées dans un répertoire	Lecture	directory*		
GetDirectoryLimits	Accorde l'autorisation d'obtenir les informations sur les limites du répertoire pour la région actuelle	Lecture			
GetSnapshotLimits	Accorde l'autorisation d'obtenir les limites des instantanés manuels pour un répertoire	Lecture	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListADAssessments	Accorde l'autorisation de répertorier les évaluations des annuaires	List			
ListAuthorizedApplications [autorisation uniquement]	Accorde l'autorisation d'obtenir les AWS applications autorisées pour un annuaire	Lecture	directory*		
ListCertificates	Accorde l'autorisation de répertorier tous les certificats enregistrés pour une connexion LDAP sécurisée, pour le répertoire spécifié	List	directory*		
ListIpRoutes	Accorde l'autorisation d'obtenir la liste des blocs d'adresses que vous avez ajoutés à un répertoire	Lecture	directory*		
ListLogSubscriptions	Accorde l'autorisation de répertorier les abonnements aux journaux actifs pour Compte AWS	Lecture			
ListSchemaExtensions	Accorde l'autorisation de répertorier toutes les extensions de schéma appliquées à un répertoire Microsoft AD	List	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier toutes les identifications sur un répertoire Amazon Directory Services	Lecture	directory*		
RegisterCertificate	Accorde l'autorisation d'enregistrer un certificat pour une connexion LDAP sécurisée	Écrire	directory*		
RegisterEventTopic	Accorde l'autorisation d'associer un répertoire à une rubrique SNS	Écrire	directory*		sns:GetTopicAttributes
RejectSharedDirectory	Accorde l'autorisation de rejeter une demande de partage de répertoire qui a été envoyée depuis le compte propriétaire du répertoire	Écrire	directory*		
RemoveIpRoutes	Accorde l'autorisation de supprimer des blocs d'adresses IP d'un répertoire	Écrire	directory*		
RemoveRegion	Accorde l'autorisation d'arrêter toutes les réplications et supprime les contrôleurs de domaine de la région spécifiée. Vous ne pouvez pas supprimer la région principale avec cette opération	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveTagsFromResource	Accorde l'autorisation de supprimer les identifications d'un répertoire Amazon Directory Services	Identification	directory*		ec2:DeleteTags
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetUserPassword	Accorde l'autorisation de réinitialiser le mot de passe de n'importe quel utilisateur de votre annuaire AWS Managed Microsoft AD ou Simple AD	Écrire	directory*		
RestoreFromSnapshot	Accorde l'autorisation de restaurer un répertoire en utilisant un instantané de répertoire existant	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ShareDirectory	Accorde l'autorisation de partager un répertoire spécifié dans votre répertoire Compte AWS (propriétaire du répertoire) avec un autre Compte AWS (consommateur du répertoire). Avec cette opération, vous pouvez utiliser votre répertoire depuis n'importe quel Compte AWS Amazon VPC au sein d'un Région AWS	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartADAssessment	Accorde l'autorisation de démarrer une évaluation de l'annuaire	Écrire			ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetwor

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					kInterfaces ec2:DescribeSubnets ec2:DescribeVpcs ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand
StartSchemaExtension	Accorde l'autorisation d'appliquer une extension de schéma à un répertoire Microsoft AD	Écrire	directory*		
UnauthorizeApplication [autorisation uniquement]	Accorde l'autorisation d'annuler l'autorisation d'une application de votre annuaire AWS	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UnshareDirectory	Accorde l'autorisation d'arrêter le partage du répertoire entre le propriétaire du répertoire et les comptes consommateurs	Écrire	directory*		
UpdateAuthorizedApplication [autorisation uniquement]	Autorise la mise à jour d'une application autorisée pour votre AWS annuaire	Écrire	directory*		
UpdateConditionalForwarder	Autorise la mise à jour d'un redirecteur conditionnel configuré pour votre annuaire AWS	Écrire	directory*		
UpdateDirectory [autorisation uniquement]	Accorde l'autorisation de mettre à jour les configurations telles que les informations d'identification du compte de service ou les adresses IP du serveur DNS pour le répertoire spécifié.	Écrire	directory*		
UpdateDirectorySetup	Accorde l'autorisation de mettre à jour le répertoire pour un type de mise à jour particulier	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateHybridAD	Accorde l'autorisation de mettre à jour les configurations pour un annuaire hybride spécifié	Écrire	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeSubnets ec2:DescribeVpcs secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNumberOfDomainControllers	Accorde l'autorisation d'ajouter des contrôleurs de domaine au répertoire ou les supprimer de ce dernier. Selon la différence entre la valeur actuelle et la nouvelle valeur (fournie via cet appel d'API), les contrôleurs de domaine seront ajoutés ou supprimés . Un nouveau contrôleur de domaine peut mettre jusqu'à 45 minutes pour devenir pleinement actif une fois que le nombre demandé de contrôleurs de domaine a été mis à jour. Pendant ce temps, vous ne pouvez pas effectuer d'autre demande de mise à jour	Écrire	directory*		
UpdateRadius	Accorde l'autorisation de mettre à jour les informations du serveur RADIUS (Remote Authentication Dial In User Service) pour un répertoire AD Connector	Écrire	directory*		
UpdateSettings	Accorde l'autorisation de mettre à jour les paramètres configurables pour le répertoire spécifié	Écrire	directory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTrust	Accorde l'autorisation de mettre à jour la confiance établie entre votre annuaire Microsoft AD AWS géré et un Active Directory local	Écrire	directory*		
VerifyTrust	Accorde l'autorisation de vérifier une relation de confiance entre votre Microsoft AD dans le AWS cloud et un domaine externe	Lecture	directory*		

Types de ressources définis par AWS Directory Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Directory Service

AWS Directory Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la valeur de la demande adressée à AWS DS	String
aws:ResourceTag/${TagKey}	Filtre l'accès par la ressource AWS DS utilisée	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les données du service de AWS répertoire

AWS Directory Service Data (préfixe de service :`ds-data`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les données du AWS Directory Service
- Types de ressources définis par AWS Directory Service Data
- Clés de condition pour les données du AWS Directory Service

Actions définies par les données du AWS Directory Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddGroupMember	Accorde l'autorisation d'ajouter un membre à un groupe dans un annuaire	Écrire	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:MemberNam ds-data:Realm ds-data:MemberRealm ds-data:Identifier	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGroup	Accorde l'autorisation de créer un groupe dans un annuaire	Écrire	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
CreateUser	Accorde l'autorisation de créer un utilisateur dans un annuaire	Écrire	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteGroup	Accorde l'autorisation de supprimer un groupe dans un annuaire	Écrire	directory*		ds:AccessDSData

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteUser	Accorde l'autorisation de supprimer un utilisateur dans un annuaire	Écrire	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeGroup	Accorde l'autorisation de décrire un groupe dans un annuaire	Lecture	directory*		ds:AccessDSData

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeUser	Accorde l'autorisation de décrire un utilisateur dans un annuaire	Lecture	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DisableUser	Accorde l'autorisation de désactiver un utilisateur dans un annuaire	Écrire	directory*		ds:AccessDSData

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
ListGroupMembers	Accorde l'autorisation de répertorier les membres d'un groupe dans un annuaire	List	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListGroups	Accorde l'autorisation de répertorier des groupes dans un annuaire	List	directory*		ds:AccessDSData
				ds-data:Realm	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGroupsForMember	Accorde l'autorisation de répertorier les groupes auxquels appartient un membre dans un annuaire	List	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListUsers	Accorde l'autorisation de répertorier les utilisateurs dans un annuaire	List	directory*		ds:AccessDSData
				ds-data:Realm	
RemoveGroupMember	Accorde l'autorisation de supprimer un membre d'un groupe dans un annuaire	Écrire	directory*		ds:AccessDSData

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ds-data:SAMAccountName ds-data:MemberNam ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
SearchGroups	Accorde l'autorisation de rechercher des groupes dans un annuaire	Lecture	directory*		ds-data:DescribeGroup ds:AccessDSData
				ds-data:Realm	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchUsers	Accorde l'autorisation de rechercher des utilisateurs dans un annuaire	Lecture	directory*		ds-data:DescribeUser ds:AccessDSData
				ds-data:Realm	
UpdateGroup	Accorde l'autorisation de mettre à jour un groupe dans un annuaire	Écrire	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
UpdateUser	Accorde l'autorisation de mettre à jour un utilisateur dans un annuaire	Écrire	directory*		ds:AccessDSData

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	

Types de ressources définis par AWS Directory Service Data

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les données du AWS Directory Service

AWS Directory Service Data définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès par la ressource AWS DS utilisée	String
ds-data:Identifier	Filtre l'accès en fonction du type d'identifiant fourni dans la demande (c'est-à-dire le nom du compte SAM)	String
ds-data:MemberName	Filtre l'accès par le nom de compte SAM du répertoire inclus dans la MemberName saisie de la demande	String
ds-data:MemberRealm	Filtre l'accès en fonction du nom de domaine du répertoire inclus dans la MemberRealm saisie de la demande	String
ds-data:Realm	Filtre l'accès en fonction du nom de domaine du répertoire pour la demande	String
ds-data:SAMAccountName	Filtre l'accès en fonction du nom de compte SAM inclus dans le SAMAccount nom saisi dans la demande	String

Actions, ressources et clés de condition pour les clusters Amazon DocumentDB Elastic

Les clusters Amazon DocumentDB Elastic (préfixe de service : `docdb-elastic`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les clusters Amazon DocumentDB Elastic
- Types de ressources définis par les clusters Amazon DocumentDB Elastic
- Clés de condition pour les clusters Amazon DocumentDB Elastic

Actions définies par les clusters Amazon DocumentDB Elastic

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApplyPendingMaintenanceAction	Accorde l'autorisation d'appliquer des actions de maintenance en attente sur le cluster Amazon DocDB-Elastic	Écrire	cluster*		
				aws:ResourceTag/${TagKey}	
CopyClusterSnapshot	Accorde l'autorisation de copier un nouvel instantané du cluster Amazon DocDB-Elastic	Écrire	cluster-snapshot*		docdb-elastic:CreateClusterSnapshot kms:CreateGrant

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					kms:Decrypt kms:DescribeKey kms:GenerateDataKey
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCluster	Accorde l'autorisation de créer un nouveau cluster Amazon DocDB-Elastic	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateClusterSnapshot	Accorde l'autorisation de créer un nouvel instantané de cluster Amazon DocDB-Elastic	Écrire	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCluster	Accorde l'autorisation de supprimer un cluster	Écrire	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteClusterSnapshot	Accorde l'autorisation de supprimer un instantané de cluster	Écrire	cluster-snapshot*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetCluster	Accorde l'autorisation d'afficher les informations d'un cluster	Lecture	cluster*		
				aws:ResourceTag/${TagKey}	
GetClusterSnapshot	Accorde l'autorisation d'afficher les informations d'un instantané de cluster	Lecture	cluster-snapshot*		
				aws:ResourceTag/${TagKey}	
GetPendingMaintenanceAction	Autorise l'accès aux informations relatives aux actions de maintenance en attente sur le cluster Amazon DocDB-Elastic	Lecture	cluster*		
				aws:ResourceTag/${TagKey}	
ListClusterSnapshots	Accorde l'autorisation de répertorier les instantanés de cluster dans votre compte	List			
ListClusters	Accorde l'autorisation de répertorier les clusters dans votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPendingMaintenanceActions	Octroie l'autorisation de répertorier les informations relatives aux actions de maintenance en cours sur n'importe quel cluster Amazon DocDB-Elastic	List		aws:ResourceTag/${TagKey}	
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource DocumentDB Elastic	List	cluster		
			cluster-snapshot		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreClusterFromSnapshot	Accorde l'autorisation de restaurer un cluster à partir d'un instantané de cluster Amazon DocDB-Elastic	Écrire	cluster*		docdb-elastic:CreateCluster ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeVpcs ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:GetSecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
StartCluster	Accorde l'autorisation de démarrer un cluster Amazon DocDB-Elastic arrêté	Écrire	cluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopCluster	Autorise l'arrêt d'un cluster Amazon DocDB-Elastic existant	Écrire	cluster*		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource DocumentDB Elastic	Identification	cluster		
			cluster-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource DocumentDB Elastic	Identification	cluster		
			cluster-snapshot		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCluster	Accorde l'autorisation de modifier un cluster	Écrire	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:ModifyVpcEndpoint kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
				aws:ResourceTag/${TagKey}	

Types de ressources définis par les clusters Amazon DocumentDB Elastic

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
cluster-snapshot	`arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster-snapshot/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les clusters Amazon DocumentDB Elastic

Les clusters Amazon DocumentDB Elastic définissent les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de paires clé-valeur de la balise dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de l'ensemble des clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon DynamoDB

Amazon DynamoDB (préfixe de service : `dynamodb`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon DynamoDB
- Types de ressources définis par Amazon DynamoDB
- Clés de condition pour Amazon DynamoDB

Actions définies par Amazon DynamoDB

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateTableReplica [autorisation uniquement]	Accorde l'autorisation de créer une réplique de table globale multi-comptes	Écrire	table*		
BatchGetItem	Accorde l'autorisation de renvoyer les attributs d'un ou de plusieurs éléments depuis une ou plusieurs tables	Lecture	table*	dynamodb:Attributes	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
BatchWriteItem	Accorde l'autorisation de placer ou supprimer plusieurs articles dans une ou plusieurs tables	Écrire	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConditionCheckItem	Accorde l'autorisation à l'ConditionCheckItem opération, vérifie l'existence d'un ensemble d'attributs pour l'élément avec la clé primaire donnée	Lecture	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
CreateBackup	Accorde l'autorisation de créer une sauvegarde pour une table existante	Écrire	table*		
CreateGlobalTable	Accorde l'autorisation de créer une table globale à partir d'une table existante	Écrire	global-table*		
			table*		
CreateGlobalTableWitness [autorisation uniquement]	Accorde l'autorisation d'ajouter un témoin à une table globale	Écrire	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTable	Autorise l' CreateTable opération : ajoute une nouvelle table à votre compte	Écrire	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTableReplica [autorisation uniquement]	Accorde l'autorisation d'ajouter une nouvelle table de réplique	Écrire	table*		
DeleteBackup	Accorde l'autorisation de supprimer une sauvegarde existante d'une table	Écrire	backup*		
DeleteGlobalTableWitness [autorisation uniquement]	Accorde l'autorisation de supprimer un témoin d'une table globale	Écrire	table*		
DeleteItem	Accorde l'autorisation de supprimer un seul élément d'une table par clé primaire	Écrire	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique basée sur les ressources attachée à la ressource	Gestion des autorisations	stream* table*		
DeleteTable	Autorise l' DeleteTable opération qui supprime une table et tous ses éléments	Écrire	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTableReplica [autorisation uniquement]	Accorde l'autorisation de supprimer une table de réplique et tous ses éléments	Écrire	table*		
DescribeBackup	Accorde l'autorisation de décrire une sauvegarde existante d'une table	Lecture	backup*		
DescribeContinuousBackups	Accorde l'autorisation de vérifier l'état des paramètres de restauration de la sauvegarde sur la table spécifiée	Lecture	table*		
DescribeContributorInsights	Accorde l'autorisation de décrire l'état des informations de type Contributor Insights et les détails associés pour une table ou un index secondaire global donné	Lecture	table* index		
DescribeEndpoints	Accorde l'autorisation de renvoyer les informations de point de terminaison régional	Lecture			
DescribeExport	Accorde l'autorisation de décrire une exportation existante d'une table	Lecture	export*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGlobalTable	Accorde l'autorisation de renvoyer des informations sur la table globale spécifiée	Lecture	global-table*		
DescribeGlobalTableSettings	Accorde l'autorisation de renvoyer des informations de paramètres sur la table globale spécifiée	Lecture	global-table*		
DescribeImport	Accorde l'autorisation de décrire une route existante	Lecture	import*		
DescribeKinesisStreamingDestination	Accorde l'autorisation de décrire l'état du streaming Kinesis et les détails associés pour une table donnée.	Lecture	table*		
DescribeLimits	Accorde l'autorisation de renvoyer les limites de capacité provisionnées actuelles pour votre région, Compte AWS à la fois pour la région dans son ensemble et pour toute table DynamoDB que vous y créez	Lecture			
DescribeReservedCapacity [autorisation uniquement]	Accorde l'autorisation de décrire une ou plusieurs capacités réservées achetées	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReservedCapacityOfferings [autorisation uniquement]	Accorde l'autorisation de décrire les offres de capacité réservée disponibles à l'achat	Lecture			
DescribeStream	Accorde l'autorisation de renvoyer des informations sur un flux, y compris l'état actuel du flux, son Amazon Resource Name (ARN), la composition de ses partitions et sa table DynamoDB correspondante	Lecture	stream*		
DescribeTable	Accorde l'autorisation de renvoyer des informations sur la table	Lecture	table*		
DescribeTableReplicaAutoScaling	Accorde l'autorisation de décrire les paramètres de scalabilité automatique pour toutes les répliques de la table globale	Lecture	table*		
DescribeTimeToLive	Accorde l'autorisation de fournir une description de l'état time-to-live (TTL) sur la table spécifiée	Lecture	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableKinesisStreamingDestination	Accorde l'autorisation d'arrêter la réplication de la table DynamoDB vers le flux de données Kinesis	Écrire	table*		
EnableKinesisStreamingDestination	Accorde l'autorisation de démarrer la réplication des données de table vers le flux de données Kinesis spécifié à l'aide d'un horodatage choisi pendant le flux d'activation	Écrire	table*		
ExportTableToPointInTime	Accorde l'autorisation de lancer une exportation d'une table DynamoDB vers S3	Écrire	table*		
GetAbacStatus [autorisation uniquement]	Accorde l'autorisation de consulter le statut du contrôle d'accès basé sur les attributs pour le compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetItem	Accorde l'autorisation à l'GetItem opération qui renvoie un ensemble d'attributs pour l'élément avec la clé primaire donnée	Lecture	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
GetRecords	Accorde l'autorisation de récupérer les enregistrements de flux d'une partition donnée	Lecture	stream*		
GetResourcePolicy	Accorde l'autorisation de consulter une politique basée sur les ressources pour une ressource	Lecture	stream*		
			table*		
GetShardIterator	Accorde l'autorisation de renvoyer un itérateur de partition	Lecture	stream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportTable	Accorde l'autorisation de lancer une exportation d'une table DynamoDB vers S3	Écrire	table*		
InjectError [autorisation uniquement]	Donne l'autorisation de démarrer des expériences sur une table globale	Écrire		dynamodb:FisActionId dynamodb:FisTargetArns	
ListBackups	Accorde l'autorisation de répertorier les sauvegardes associées au compte et au point de terminaison	List			
ListContributorInsights	Accorde l'autorisation de répertorier ContributorInsightsSummary pour toutes les tables et les index secondaires globaux associés au compte courant et au point de terminaison	List			
ListExports	Accorde l'autorisation de répertorier les exportations associées au compte et au point de terminaison	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGlobalTables	Accorde l'autorisation de répertorier toutes les tables globales ayant une réplique dans la région spécifiée	List			
ListImports	Accorde l'autorisation de répertorier les sauvegardes associées au compte et au point de terminaison	List			
ListStreams	Autorise le renvoi d'un tableau de flux ARNs associés au compte courant et au point de terminaison	Lecture			
ListTables	Accorde l'autorisation de renvoyer un tableau des noms de tables associés au compte et au point de terminaison actuels	List			
ListTagsOfResource	Accorde l'autorisation de répertorier toutes les balises d'une ressource Amazon DynamoDB	Lecture	table*		
PartiQLDelete	Accorde l'autorisation de supprimer un seul élément d'une table par clé primaire.	Écriture	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PartiQLInsert	Accorde l'autorisation de créer un nouvel élément si un élément avec la même clé primaire n'existe pas dans la table.	Écriture	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys	
PartiQLSelect	Accorde l'autorisation de lire un ensemble d'attributs pour les éléments d'une table ou d'un index.	Lecture	table*		
			index		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:FullTableScan dynamodb:LeadingKeys dynamodb:Select	
PartiQLUpdate	Accorde l'autorisation de modifier des attributs d'un élément existant.	Écrire	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PurchaseReservedCapacityOfferings [autorisation uniquement]	Accorde l'autorisation d'acheter une capacité réservée à utiliser avec votre compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutItem	Accorde l'autorisation de créer un élément ou de remplacer un ancien élément par un nouveau	Écrire	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
PutResourcePolicy	Accorde l'autorisation d'associer une politique basée sur les ressources à la ressource	Gestion des autorisations	stream*		
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Query	Accorde l'autorisation d'utiliser la clé primaire d'une table ou d'un index secondaire afin d'accéder directement aux éléments depuis cette table ou cet index	Lecture	table*		
			index		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
ReadDataForReplication [autorisation uniquement]	Accorde l'autorisation de lire les données d'une réplique de table globale multi-comptes	Lecture	table*		
ReplicateSettings [autorisation uniquement]	Accorde l'autorisation de configurer les paramètres d'une réplique de table globale multi-comptes	Écrire	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreTableFromAwsBackup [autorisation uniquement]	Autorise la création d'une nouvelle table à partir du point de restauration sur AWS Backup	Écrire	table*		
RestoreTableFromBackup	Accorde l'autorisation de créer une table à partir d'une sauvegarde existante	Écrire	backup*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreTableToPointInTime	Accorde l'autorisation de restaurer une table sur un point dans le temps	Écrire	table*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Scan	Accorde l'autorisation de renvoyer un ou plusieurs éléments et attributs d'élément en accédant à chaque élément dans une table ou un index secondaire	Lecture	table*		
			index		
				dynamodb:Attributes dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
StartAwsBackupJob [autorisation uniquement]	Autorise la création d'une sauvegarde sur AWS Backup avec les fonctionnalités avancées activées	Écrire	table*		
TagResource	Accorde l'autorisation d'associer un ensemble de balises à une ressource Amazon DynamoDB	Identification	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer l'association de balises d'une ressource Amazon DynamoDB	Identification	table*		
				aws:TagKeys	
UpdateAbacStatus [autorisation uniquement]	Accorde l'autorisation de mettre à jour le statut du contrôle d'accès basé sur les attributs pour le compte	Gestion des autorisations			
UpdateContinuousBackups	Accorde l'autorisation d'activer ou de désactiver des sauvegardes continues	Écrire	table*		
UpdateContributorInsights	Accorde l'autorisation de mettre à jour le statut des informations de type Contributor Insights pour une table ou un index secondaire global spécifique	Écrire	table*		
			index		
UpdateGlobalTable	Accorde l'autorisation d'ajouter ou de supprimer des répliques dans la table globale spécifiée	Écrire	global-table*		
			table*		
UpdateGlobalTableSettings	Accorde l'autorisation de mettre à jour les paramètres de la table globale spécifiée	Écrire	global-table*		
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGlobalTableVersion [autorisation uniquement]	Accorde l'autorisation de mettre à jour la version de la table globale spécifiée	Écrire	global-table*		
			table		
UpdateItem	Accorde l'autorisation de modifier les attributs d'un élément existant, ou d'ajouter un nouvel élément à la table si celui-ci n'existe pas déjà	Écrire	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateKinesisStreamingDestination	Accorde l'autorisation de mettre à jour les configurations de réplication des données pour le flux de données Kinesis spécifié	Écrire	table*		
UpdateTable	Accorde l'autorisation de modifier les paramètres de débit alloué, les index secondaires globaux ou les paramètres DynamoDB Streams pour une table donnée	Écrire	table*		
UpdateTableReplicaAutoScaling	Accorde l'autorisation de mettre à jour les paramètres de scalabilité automatique de votre table de réplique	Écrire	table*		
UpdateTimeToLive	Accorde l'autorisation d'activer ou de désactiver le protocole TTL pour la table spécifiée	Écrire	table*		
WriteDataForReplication [autorisation uniquement]	Accorde l'autorisation d'écrire des données dans une réplique de table globale multi-comptes	Écrire	table*		

Types de ressources définis par Amazon DynamoDB

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
index	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/stream/${StreamLabel}`	
table	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/backup/${BackupName}`	
export	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/export/${ExportName}`	
global-table	`arn:${Partition}:dynamodb::${Account}:global-table/${GlobalTableName}`	
import	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/import/${ImportName}`	

Clés de condition pour Amazon DynamoDB

Amazon DynamoDB définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

> **Note**
>
> Pour de plus amples informations sur l'utilisation des clés de contexte pour affiner l'accès à DynamoDB à l'aide d'une politique IAM, veuillez consulter Utilisation de conditions de politique IAM pour un contrôle précis des accès dans le Guide du développeur Amazon DynamoDB.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
dynamodb:Attributes	Filtre l'accès en fonction des noms d'attribut (champ ou colonne) de la table	ArrayOfString
dynamodb:EnclosingOperation	Filtre l'accès en bloquant les APIs appels liés aux transactions et en autorisant les APIs appels non transactionnels et vice-versa	String

Clés de condition	Description	Type
dynamodb:FirstPartitionKeyValues	Filtre l'accès en fonction de la première clé de partition de la table	ArrayOfString
dynamodb:FisActionId	Filtre l'accès en fonction de l'ID d'une AWS action FIS	String
dynamodb:FisTargetArns	Filtre l'accès par l'ARN d'une AWS cible FIS	ArrayOfARN
dynamodb:FourthPartitionKeyValues	Filtre l'accès par la quatrième clé de partition de la table	ArrayOfString
dynamodb:FullTableScan	Filtre l'accès en bloquant l'analyse complète du tableau	Booléen
dynamodb:LeadingKeys	Filtre l'accès en fonction de la première clé de partition de la table	ArrayOfString
dynamodb:ReturnConsumedCapacity	Filtre l'accès en fonction du ReturnConsumedCapacity paramètre d'une demande. Contient « TOTAL » ou « NONE »	String
dynamodb:ReturnValues	Filtre l'accès en fonction du ReturnValues paramètre de demande. Contient l'un des éléments suivants : « ALL_OLD », « UPDATED_OLD »,« ALL_NEW », « UPDATED_NEW » ou « NONE »	String
dynamodb:SecondPartitionKeyValues	Filtre l'accès par la deuxième clé de partition de la table	ArrayOfString
dynamodb:Select	Filtre l'accès en fonction du paramètre Select d'une requête d'une demande d'analyse	String

Clés de condition	Description	Type
dynamodb:ThirdPartitionKeyValues	Filtre l'accès par la troisième clé de partition de la table	ArrayOfString

Actions, ressources et clés de condition pour Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) (préfixe de service : `dax`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon DynamoDB Accelerator (DAX)
- Types de ressources définis par Amazon DynamoDB Accelerator (DAX)
- Clés de condition pour Amazon DynamoDB Accelerator (DAX)

Actions définies par Amazon DynamoDB Accelerator (DAX)

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetItem	Accorde l'autorisation de renvoyer les attributs d'un ou de plusieurs éléments depuis une ou plusieurs tables	Lecture	application*		
BatchWriteItem	Accorde l'autorisation de placer ou supprimer plusieurs articles dans une ou plusieurs tables	Écrire	application*		
ConditionCheckItem	Accorde l'autorisation à l'ConditionCheckItem opération qui vérifie l'existence d'un ensemble d'attributs pour l'élément avec la clé primaire donnée	Lecture	application*		
CreateCluster	Accorde l'autorisation de créer un cluster DAX	Écrire	application*		dax:CreateParameterGroup dax:CreateSubnetGroup ec2:CreateNetworkInterface ec2:DeleteNetworkInterface

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole iam:PassRole
CreateParameterGroup	Accorde l'autorisation de créer un groupe de paramètres.	Écrire			
CreateSubnetGroup	Accorde l'autorisation de créer un groupe de sous-réseaux	Écrire			
DecreaseReplicationFactor	Accorde l'autorisation de supprimer un ou plusieurs nœuds d'un cluster DAX	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCluster	Accorde l'autorisation de supprimer un cluster DAX précédemment provisionné	Écrire	application*		
DeleteItem	Accorde l'autorisation de supprimer un seul élément d'une table par clé primaire.	Écrire	application*		
				dax:EnclosingOperation	
DeleteParameterGroup	Accorde l'autorisation de supprimer le groupe de paramètres spécifié	Écrire			
DeleteSubnetGroup	Accorde l'autorisation de supprimer un groupe de sous-réseaux	Écrire			
DescribeClusters	Accorde l'autorisation de renvoyer des informations sur tous les clusters DAX provisionnés	List	application		
DescribeDefaultParameters	Accorde l'autorisation de renvoyer les informations sur les paramètres système par défaut pour DAX	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEvents	Accorde l'autorisation de renvoyer les événements liés aux clusters DAX et aux groupes de paramètres	List			
DescribeParameterGroups	Accorde l'autorisation de renvoyer une liste de descriptions de groupe de paramètres	List			
DescribeParameters	Accorde l'autorisation de renvoyer la liste détaillée des paramètres pour un groupe de paramètres particulier	Lecture			
DescribeSubnetGroups	Accorde l'autorisation de renvoyer une liste de descriptions de groupe de sous-réseau	List			
GetItem	Accorde l'autorisation à l'GetItem opération qui renvoie un ensemble d'attributs pour l'élément avec la clé primaire donnée	Lecture	application*		
				dax:EnclosingOperation	
IncreaseReplicationFactor	Accorde l'autorisation d'ajouter un ou plusieurs nœuds à un cluster DAX	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTags	Accorde l'autorisation de renvoyer une liste de toutes les identifications d'un cluster DAX	Lecture	application*		
PutItem	Accorde l'autorisation de créer un élément ou de remplacer un ancien élément par un nouveau	Écrire	application*		
				dax:EnclosingOperation	
Query	Accorde l'autorisation d'utiliser la clé primaire d'une table ou d'un index secondaire afin d'accéder directement aux éléments depuis cette table ou cet index	Lecture	application*		
RebootNode	Accorde l'autorisation de redémarrer un seul nœud d'un cluster DAX	Écrire	application*		
Scan	Accorde l'autorisation de renvoyer un ou plusieurs éléments et attributs d'élément en accédant à chaque élément dans une table ou un index secondaire	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'associer un jeu d'identifications à une ressource DAX	Identification	application*		
UntagResource	Accorde l'autorisation de supprimer l'association d'identifications d'une ressource DAX	Identification	application*		
UpdateCluster	Accorde l'autorisation de modifier les paramètres d'un cluster DAX	Écrire	application*		
UpdateItem	Accorde l'autorisation de modifier les attributs d'un élément existant, ou d'ajouter un nouvel élément à la table si celui-ci n'existe pas déjà	Écrire	application*		
				dax:EnclosingOperation	
UpdateParameterGroup	Accorde l'autorisation de modifier les paramètres d'un groupe de paramètres	Écrire			
UpdateSubnetGroup	Accorde l'autorisation de modifier un groupe de sous-réseaux existant	Écrire			

Types de ressources définis par Amazon DynamoDB Accelerator (DAX)

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Clés de condition pour Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
dax:EnclosingOperation	Utilisé pour bloquer les APIs appels de transactions et autoriser les APIs appels non transactionnels et vice-versa	String

Actions, ressources et clés de condition pour Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling (préfixe de service : `autoscaling`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définie par Amazon EC2 Auto Scaling
- Types de ressources définis par Amazon EC2 Auto Scaling
- Clés de condition pour Amazon EC2 Auto Scaling

Actions définie par Amazon EC2 Auto Scaling

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AttachInstances	Accorde l'autorisation d'attacher une ou plusieurs instances EC2 au groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
AttachLoadBalancerTargetGroups	Accorde l'autorisation d'attacher un ou plusieurs groupes cibles au groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	
AttachLoadBalancers	Accorde l'autorisation d'attacher un ou plusieurs équilibreurs de charge au groupe Auto Scaling spécifié.	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
AttachTrafficSources	Accorde l'autorisation d'attacher une ou plusieurs sources de trafic à un groupe Auto Scaling	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				autoscaling:TrafficSourceIdentifiers	
BatchDeleteScheduledAction	Accorde l'autorisation de supprimer les actions planifiées spécifiées	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
BatchPutScheduledUpdateGroupAction	Accorde l'autorisation de créer ou de mettre à jour plusieurs actions de scalabilité planifiées pour un groupe Auto Scaling.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelInstanceRefresh	Accorde l'autorisation d'annuler une opération d'actualisation d'instance en cours	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CompleteLifecycleAction	Accorde l'autorisation de terminer l'action du cycle de vie pour le jeton spécifié ou l'instance spécifiée avec le résultat spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateAutoScalingGroup	Accorde l'autorisation de créer un groupe Auto Scaling avec le nom et les attributs spécifiés .	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				autoscaling:ImageId autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				autoscaling:LoadBalancerNames autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLaunchConfiguration	Accorde l'autorisation de créer une configuration de lancement.	Écriture	launchConfiguration*		
				autoscaling:ImageId autoscaling:InstanceType autoscaling:SpotPrice autoscaling:MetadataHttpTokens autoscaling:MetadataHttpPutResponseHopLimit autoscaling:MetadataHttpEndpoint	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOrUpdateTags	Accorde l'autorisation de créer ou de mettre à jour des balises pour le groupe Auto Scaling spécifié	Balisage	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	Accorde l'autorisation de supprimer le groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ForceDelete autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLaunchConfiguration	Accorde l'autorisation de supprimer la configuration de lancement spécifiée.	Écriture	launchConfiguration*		
DeleteLifecycleHook	Accorde l'autorisation de supprimer le hook de cycle de vie spécifié	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotificationConfiguration	Accorde l'autorisation de supprimer la notification spécifiée	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePolicy	Accorde l'autorisation de supprimer la politique Auto Scaling spécifiée	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteScheduledAction	Accorde l'autorisation de supprimer l'action planifiée spécifiée	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	Accorde l'autorisation de supprimer les balises spécifiées	Balisage	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWarmPool	Accorde l'autorisation de supprimer le groupe « à chaud » associé au groupe Auto Scaling	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	Accorde l'autorisation de décrire les limites de ressources actuelles d'Auto Scaling pour votre Compte AWS	List			
DescribeAccountSettings	Accorde l'autorisation de décrire les paramètres actuels du compte Amazon EC2 Auto Scaling pour votre compte	List			
DescribeAdjustmentTypes	Accorde l'autorisation de décrire les types d'ajustement des politiques à utiliser avec PutScalingPolicy	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAutoScalingGroups	Accorde l'autorisation de décrire un ou plusieurs groupes Auto Scaling. Si la liste des noms n'est pas fournie, l'appel décrit tous les groupes Auto Scaling.	Liste			
DescribeAutoScalingInstances	Accorde l'autorisation de décrire une ou plusieurs instances Auto Scaling. Si la liste n'est pas fournie, l'appel décrit toutes les instances.	Liste			
DescribeAutoScalingNotificationTypes	Accorde l'autorisation de décrire les types de notification pris en charge par Auto Scaling.	Liste			
DescribeInstanceRefreshes	Accorde l'autorisation de décrire une ou plusieurs actualisations d'instance pour un groupe Auto Scaling	Liste			
DescribeLaunchConfigurations	Accorde l'autorisation de décrire une ou plusieurs configurations de lancement. Si vous omettez la liste des noms, l'appel décrit toutes les configurations de lancement.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeLifecycleHookTypes	Accorde l'autorisation de décrire les types de hooks de cycle de vie disponibles.	Liste			
DescribeLifecycleHooks	Accorde l'autorisation de décrire les hooks de cycle de vie pour le groupe Auto Scaling spécifié.	Liste			
DescribeLoadBalancerTargetGroups	Accorde l'autorisation de décrire les groupes cibles pour le groupe Auto Scaling spécifié.	Liste			
DescribeLoadBalancers	Accorde l'autorisation de décrire les équilibreurs de charge pour le groupe Auto Scaling spécifié.	List			
DescribeMetricCollectionTypes	Accorde l'autorisation de décrire les CloudWatch métriques disponibles pour Auto Scaling	List			
DescribeNotificationConfigurations	Accorde l'autorisation de décrire les actions de notification associées au groupe Auto Scaling spécifié.	Liste			
DescribePolicies	Accorde l'autorisation de décrire les stratégies pour le groupe Auto Scaling spécifié.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeScalingActivities	Accorde l'autorisation de décrire une ou plusieurs activités de scalabilité pour le groupe Auto Scaling spécifié.	List			
DescribeScalingProcessTypes	Accorde l'autorisation de décrire les types de processus de dimensionnement à utiliser avec ResumeProcesses et SuspendProcesses	List			
DescribeScheduledActions	Accorde l'autorisation de décrire les actions planifiées pour votre groupe Auto Scaling qui n'ont pas été exécutées.	Liste			
DescribeTags	Accorde l'autorisation pour décrire les balises spécifiées	Lecture			
DescribeTerminationPolicyTypes	Accorde l'autorisation de décrire les stratégies de mise hors service prises en charge par Auto Scaling.	List			
DescribeTrafficSources	Accorde l'autorisation de décrire les groupes cibles pour le groupe Auto Scaling spécifié.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWarmPool	Accorde l'autorisation de décrire le groupe « à chaud » associé au groupe Auto Scaling	Liste			
DetachInstances	Accorde l'autorisation de supprimer une ou plusieurs instances du groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DetachLoadBalancerTargetGroups	Accorde l'autorisation de détacher un ou plusieurs groupes cibles du groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DetachLoadBalancers	Accorde l'autorisation de supprimer un ou plusieurs équilibreurs de charge du groupe Auto Scaling spécifié.	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
DetachTrafficSources	Accorde l'autorisation de détacher une ou plusieurs sources de trafic d'un groupe Auto Scaling	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableMetricsCollection	Accorde l'autorisation de désactiver la surveillance des métriques spécifiées pour le groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnableMetricsCollection	Accorde l'autorisation d'activer la surveillance des métriques spécifiées pour le groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnterStandby	Accorde l'autorisation de déplacer les instances spécifiées en mode en veille	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExecutePolicy	Accorde l'autorisation d'exécuter la politique spécifiée.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExitStandby	Accorde l'autorisation de placer les instances spécifiées hors du mode en veille.	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	Accorde l'autorisation de récupérer les données de prévision pour une politique de mise à l'échelle prédictive	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
LaunchInstances	Accorde l'autorisation de lancer une ou plusieurs instances EC2 dans le groupe Auto Scaling spécifié	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutAccountSetting	Accorde l'autorisation de modifier un paramètre de compte pour votre compte	Écrire			
PutLifecycleHook	Accorde l'autorisation de créer ou de mettre à jour un hook de cycle de vie pour le groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutNotificationConfiguration	Accorde l'autorisation de configurer un groupe Auto Scaling pour envoyer des notifications lorsque les événements spécifiés se produisent.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	Accorde l'autorisation de créer ou de mettre à jour d'une politique pour un groupe Auto Scaling	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScheduledUpdateGroupAction	Accorde l'autorisation de créer ou de mettre à jour une action de scalabilité planifiée pour un groupe Auto Scaling.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	Accorde l'autorisation de créer ou de mettre à jour le groupe « à chaud » associé au groupe Auto Scaling spécifié	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RecordLifecycleActionHeartbeat	Accorde l'autorisation d'enregistrer une pulsation pour l'action de cycle de vie associée au jeton spécifié ou à l'instance spécifiée.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResumeProcesses	Accorde l'autorisation de reprendre les processus Auto Scaling suspendus spécifiés, ou tous les processus suspendus, pour le groupe Auto Scaling spécifié.	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	Accorde l'autorisation d'annuler une opération d'actualisation d'instance en cours	Écrire	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetDesiredCapacity	Accorde l'autorisation de définir la taille du groupe Auto Scaling spécifié	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetInstanceHealth	Accorde l'autorisation de définir le statut de santé de l'instance spécifiée	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	Accorde l'autorisation de mettre à jour les paramètres de protection d'instance des instances spécifiées	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartInstanceRefresh	Accorde l'autorisation de démarrer une nouvelle opération d'actualisation d'instance	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				autoscaling:ImageId	
SuspendProcesses	Accorde l'autorisation de suspendre les processus Auto Scaling spécifiés, ou tous les processus, pour le groupe Auto Scaling spécifié.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	Accorde l'autorisation de résilier l'instance spécifiée et d'ajuster éventuellement la taille de groupe souhaitée.	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAutoScalingGroup	Accorde l'autorisation de mettre à jour la configuration pour le groupe Auto Scaling spécifié	Écriture	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				autoscaling:ImageId autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				autoscaling:MaxSize autoscaling:MinSize autoscaling:VPCZoneIdentifiers	

Types de ressources définis par Amazon EC2 Auto Scaling

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
autoScalingGroup	`arn:${Partition}:autoscaling:${Region}:${Account}:autoScalingGroup:${GroupId}:autoScalingGroupName/${GroupFriendlyName}`	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
launchConfiguration	`arn:${Partition}:autoscaling:${Region}:${Account}:launchConfiguration:${Id}:launchConfigurationName/${LaunchConfigurationName}`	

Clés de condition pour Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
autoscaling:CapacityReservationIds	Filtre l'accès en fonction de la réservation de capacité IDs	ArrayOfString
autoscaling:CapacityReservationResourceGroupArns	Filtre l'accès en fonction de l'ARN d'un groupe de ressources de réservation de capacité	ArrayOfString
autoscaling:ForceDelete	Filtre l'accès selon que l'option de suppression forcée est spécifiée ou non lors de la suppression d'un groupe Auto Scaling	Booléen
autoscaling:ImageId	Filtre l'accès en fonction de l'ID de l'AMI d'une configuration de lancement	String

Clés de condition	Description	Type
autoscaling:InstanceType	Filtre l'accès en fonction du type d'instance pour la configuration de lancement	String
autoscaling:InstanceTypes	Filtre l'accès en fonction des types d'instances présents en tant que substitutions à un modèle de lancement pour une politique d'instances mixtes. Utilisez-le pour déterminer quels types d'instances peuvent être définis explicitement dans la politique	String
autoscaling:LaunchConfigurationName	Filtre l'accès en fonction du nom d'une configuration de lancement	Chaîne
autoscaling:LaunchTemplateVersionSpecified	Filtre l'accès selon que les utilisateurs peuvent spécifier ou non n'importe quelle version d'un modèle de lancement ou uniquement la dernière version ou la version par défaut	Booléen
autoscaling:LoadBalancerNames	Filtre l'accès en fonction du nom de l'équilibreur de charge	ArrayOfString
autoscaling:MaxSize	Filtre l'accès en fonction de la taille maximale de mise à l'échelle dans la requête	Numérique
autoscaling:MetadataHttpEndpoint	Filtre l'accès selon que le point de terminaison HTTP est activé ou non pour le service de métadonnées d'instance.	Chaîne
autoscaling:MetadataHttpPutResponseHopLimit	Filtre l'accès en fonction du nombre autorisé de sauts lors de l'appel du service de métadonnées d'instance.	Numérique

Clés de condition	Description	Type
autoscaling:MetadataHttpTokens	Filtre l'accès selon que des jetons sont requis ou non lors de l'appel du service de métadonnées d'instance (facultatif ou obligatoire).	String
autoscaling:MinSize	Filtre l'accès en fonction de la taille minimale de mise à l'échelle dans la requête	Numérique
autoscaling:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String
autoscaling:SpotPrice	Filtre l'accès en fonction du prix des instances Spot pour la configuration de lancement	Numérique
autoscaling:TargetGroupARNs	Filtre l'accès en fonction de l'ARN d'un groupe cible	ArrayOfARN
autoscaling:TrafficSourceIdentifiers	Filtre l'accès en fonction des identifiants des sources de trafic	ArrayOfString
autoscaling:VPCZoneIdentifiers	Filtre l'accès en fonction de l'identificateur d'une zone VPC	ArrayOfString
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon EC2 Image Builder

Amazon EC2 Image Builder (préfixe de service : `imagebuilder`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EC2 Image Builder
- Types de ressources définis par Amazon EC2 Image Builder
- Clés de condition pour Amazon EC2 Image Builder

Actions définies par Amazon EC2 Image Builder

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelImageCreation	Accorde l'autorisation d'annuler la création d'une image	Écrire	image*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelLifecycleExecution	Octroie l'autorisation d'annuler l'exécution d'un cycle de vie.	Écrire	lifecycleExecution*		
CreateComponent	Accorde l'autorisation de créer un composant	Écriture	component*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateContainerRecipe	Accorde l'autorisation de créer une recette de conteneur	Écriture	containerRecipe*		ec2:DescribeImages ecr:DescribeImages ecr:DescribeRepositories imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					s3:GetObject s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDistributionConfiguration	Accorde l'autorisation de créer une configuration de distribution	Écriture	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate imagebuilder:TagResource s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateImage	Accorde l'autorisation de créer une image	Écriture	image*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateImagePipeline	Accorde l'autorisation de créer un pipeline d'images	Écriture	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateImageRecipe	Accorde l'autorisation de créer une recette d'image	Écriture	imageRecipe*		ec2:DescribeImages imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInfrastructureConfiguration	Accorde l'autorisation de créer une configuration d'infrastructure	Écrire	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole imagebuilder:TagResource resource-groups:GetGroup sns:Publish

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLifecyclePolicy	Octroie l'autorisation de créer une stratégie de cycle de vie.	Écrire	lifecyclePolicy*		iam:PassRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkflow	Accorde l'autorisation de créer un nouveau flux de travail	Écrire	workflow*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponent	Accorde l'autorisation de supprimer un composant	Écriture	component*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteContainerRecipe	Accorde l'autorisation de supprimer une recette de conteneur	Écriture	containerRecipe*		
DeleteDistributionConfiguration	Accorde l'autorisation de supprimer une configuration de distribution	Écriture	distributionConfiguration*		
DeleteImage	Accorde l'autorisation de supprimer une image	Écriture	image*		
DeleteImagePipeline	Accorde l'autorisation de supprimer un pipeline d'images	Écriture	imagePipeline*		
DeleteImageRecipe	Accorde l'autorisation de supprimer une recette d'image	Écriture	imageRecipe*		
DeleteInfrastructureConfiguration	Accorde l'autorisation de supprimer une configuration d'infrastructure	Écrire	infrastructureConfiguration*		
DeleteLifecyclePolicy	Accorde l'autorisation de supprimer une politique de cycle de vie	Écrire	lifecyclePolicy*		
DeleteWorkflow	Accorde l'autorisation de supprimer un flux de travail.	Écrire	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DistributeImage	Autorise la diffusion d'une image	Écrire	image*		ec2:DescribeImages iam:PassRole imagebuilder:GetDistributionConfiguration imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	
GetComponent	Accorde l'autorisation d'afficher les informations sur un composant	Lecture	component*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetComponentPolicy	Accorde l'autorisation d'afficher la politique de ressource associée à un composant	Lecture	component*		
GetContainerRecipe	Accorde l'autorisation d'afficher les détails d'une recette de conteneur	Lecture	containerRecipe*		
GetContainerRecipePolicy	Accorde l'autorisation d'afficher la politique de ressource associée à une recette de conteneur	Lecture	containerRecipe*		
GetDistributionConfiguration	Accorde l'autorisation d'afficher les détails d'une configuration de distribution	Lecture	distributionConfiguration*		
GetImage	Accorde l'autorisation d'afficher les détails d'une image	Lecture	image*		
GetImagePipeline	Accorde l'autorisation d'afficher les détails d'un pipeline d'images	Lecture	imagePipeline*		
GetImagePolicy	Accorde l'autorisation d'afficher la politique de ressource associée à une image	Lecture	image*		
GetImageRecipe	Accorde l'autorisation d'afficher les détails d'une recette d'image	Lecture	imageRecipe*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetImageRecipePolicy	Accorde l'autorisation d'afficher la politique de ressource associée à une recette d'image	Lecture	imageRecipe*		
GetInfrastructureConfiguration	Accorde l'autorisation d'afficher les détails d'une configuration d'infrastructure	Lecture	infrastructureConfiguration*		
GetLifecycleExecution	Octroie l'autorisation d'afficher les informations sur l'exécution d'un cycle de vie.	Lecture	lifecycleExecution*		
GetLifecyclePolicy	Octroie l'autorisation d'afficher les informations sur une stratégie de cycle de vie.	Lecture	lifecyclePolicy*		
GetMarketplaceResource	Accorde l'autorisation de récupérer la ressource fournie par Marketplace	Lecture	component*		
GetWorkflow	Accorde l'autorisation d'afficher les informations sur un flux de travail	Lecture	workflow*		kms:Decrypt
GetWorkflowExecution	Accorde l'autorisation d'afficher les informations sur l'exécution d'un flux de travail	Lecture	workflowExecution*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkflowStepExecution	Accorde l'autorisation d'afficher les informations sur l'exécution des étapes du flux de travail	Lecture	workflowStepExecution*		kms:Decrypt
ImportComponent	Accorde l'autorisation d'importer un nouveau composant	Écrire	component*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportDiskImage	Accorde l'autorisation d'importer une image disque	Écrire	imageVersion*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportVmImage	Accorde l'autorisation d'importer une image	Écrire	imageVersion*		ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
ListComponentBuildVersions	Accorde l'autorisation de répertorier les versions de génération de composants dans votre compte	Liste	allComponentBuildVersions*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListComponents	Accorde l'autorisation de répertorier les versions de composants appartenant à votre compte ou partagées avec celui-ci	Liste			
ListContainerRecipes	Accorde l'autorisation de répertorier les recettes de conteneur appartenant à votre compte ou partagées avec celui-ci	Liste			
ListDistributionConfigurations	Accorde l'autorisation de répertorier les configurations de distribution de votre compte	Liste			
ListImageBuildVersions	Accorde l'autorisation de répertorier les versions de génération d'images dans votre compte	List	allImageBuildVersions*		
ListImagePackages	Accorde l'autorisation de retourner une liste de packages installés sur l'image spécifiée	List	image*		
ListImagePipelineImages	Accorde l'autorisation de retourner une liste d'images créés par le pipeline spécifié	List	imagePipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListImagePipelines	Accorde l'autorisation de répertorier les pipelines d'images dans votre compte	Liste			
ListImageRecipes	Accorde l'autorisation de répertorier les recettes d'image appartenant à votre compte ou partagées avec celui-ci	List			
ListImageScanFindingAggregations	Accorde l'autorisation de répertorier les agrégations sur les résultats de numérisation d'images dans votre compte	List	image		
			imagePipeline		
ListImageScanFindings	Accorde l'autorisation de répertorier les résultats de numérisation d'images dans votre compte	List	image		inspector2:ListFindings
			imagePipeline		
ListImages	Accorde l'autorisation de répertorier les versions d'image appartenant à votre compte ou partagées avec celui-ci	Liste			
ListInfrastructureConfigurations	Accorde l'autorisation de répertorier les configurations d'infrastructure de votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLifecycleExecutionResources	Octroie l'autorisation de répertorier des ressources pour l'exécution du cycle de vie spécifié.	List	lifecycleExecution*		
ListLifecycleExecutions	Octroie l'autorisation de répertorier des exécutions pour la ressource spécifiée.	List	image		
			lifecyclePolicy		
ListLifecyclePolicies	Octroie l'autorisation de répertorier les stratégies de cycle de vie de votre compte.	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications pour une ressource Image Builder	Lecture	component		
			containerRecipe		
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
ListWaitingWorkflowSteps	Accorde l'autorisation de répertorier les étapes du flux de travail en attente pour le compte de l'appelant	List			
ListWorkflowBuildVersions	Accorde l'autorisation de répertorier les versions de génération de flux de travail dans votre compte	List	allWorkflowBuildVersions*		
ListWorkflowExecutions	Accorde l'autorisation de répertorier les exécutions de flux de travail de l'image spécifiée	List	image*		
ListWorkflowStepExecutions	Accorde l'autorisation de répertorier les exécutions des étapes du flux de travail spécifié	List	workflowExecution*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWorkflows	Accorde l'autorisation de répertorier les versions de flux de travail appartenant à votre compte ou partagées avec celui-ci	List			
PutComponentPolicy	Accorde l'autorisation de définir la politique de ressource associée à un composant	Gestion des autorisations	component*		
PutContainerRecipePolicy	Accorde l'autorisation de définir la politique de ressource associée à une recette de conteneur	Gestion des autorisations	containerRecipe*		
PutImagePolicy	Accorde l'autorisation de définir la politique de ressource associée à une image	Gestion des autorisations	image*		
PutImageRecipePolicy	Accorde l'autorisation de définir la politique de ressource associée à une recette d'image	Gestion des autorisations	imageRecipe*		
RetryImage	Accorde l'autorisation de réessayer de créer une image	Écrire	image*		
SendWorkflowStepAction	Accorde l'autorisation d'envoyer une action à une étape du flux de travail	Écrire	image*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workflowStepExecution*		
StartImagePipelineExecution	Accorde l'autorisation de créer une image à partir d'un pipeline	Écrire	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartResourceStateUpdate	Octroie l'autorisation de lancer une mise à jour de l'état pour la ressource spécifiée.	Écrire	image*		
TagResource	Accorde l'autorisation d'identificationr une ressource Image Builder	Balisage	component		
			containerRecipe		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer la balise d'une ressource Image Builder	Balisage	component		
			containerRecipe		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDistributionConfiguration	Accorde l'autorisation de mettre à jour une configuration de distribution existante	Écriture	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate s3:ListBucket ssm:GetParameter

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateImagePipeline	Accorde l'autorisation de mettre à jour un pipeline d'images existant	Écriture	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow inspector2:BatchGetAccountStatus
UpdateInfrastructureConfiguration	Accorde l'autorisation de mette à jour une configuration d'infrastructure existante	Écrire	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole resource-groups:GetGroup sns:Publish

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	
UpdateLifecyclePolicy	Octroie l'autorisation de mettre à jour une stratégie de cycle de vie existante.	Écrire	lifecyclePolicy*		iam:PassRole
				imagebuilder:LifecyclePolicyResourceType	

Types de ressources définis par Amazon EC2 Image Builder

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
component	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}`	aws:ResourceTag/${TagKey}
distributionConfiguration	`arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}`	aws:ResourceTag/${TagKey}
imageVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}`	aws:ResourceTag/${TagKey}
imageRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}`	aws:ResourceTag/${TagKey}
containerRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}	
workflowStepExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}	
allComponentBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/*	

Types de ressources	ARN	Clés de condition
allImageBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/*	
allWorkflowBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/*	

Clés de condition pour Amazon EC2 Image Builder

Amazon EC2 Image Builder définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
imagebuilder:Creat	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource créée par Image Builder	Chaîne

Clés de condition	Description	Type
edResourceTag/${TagKey}		
imagebuilder:CreatedResourceTagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
imagebuilder:Ec2MetadataHttpTokens	Filtre l'accès par l'exigence du jeton HTTP de métadonnées de l'instance EC2 spécifiée dans la requête.	String
imagebuilder:LifecyclePolicyResourceType	Filtre l'accès en fonction du type de ressource de stratégie de cycle de vie spécifié dans la demande.	String
imagebuilder:StatusTopicArn	Filtre l'accès par l'ARN de la rubrique SNS dans la requête où les notifications d'état du terminal seront publiées	ARN

Actions, ressources et clés de condition pour Amazon EC2 Instance Connect

Amazon EC2 Instance Connect (préfixe de service : `ec2-instance-connect`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EC2 Instance Connect
- Types de ressources définis par Amazon EC2 Instance Connect
- Clés de condition pour Amazon EC2 Instance Connect

Actions définies par Amazon EC2 Instance Connect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
OpenTunnel	Accorde l'autorisation de mettre en place une connexion SSH vers une instance EC2 à l'aide du point de terminaison d'EC2 Instance Connect	Écrire	instance-connect-endpoint*		
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2-instance-connect:remotePort	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ec2-instance-connect:privateIpAddress ec2-instance-connect:MaxTunnelDuration	
SendSSHPublicKey	Octroie l'autorisation de transmettre une clé publique SSH à l'instance EC2 spécifiée qui sera utilisée pour un SSH standard.	Écrire	instance*		
				ec2:osuser	
SendSerialConsoleSSHPublicKey	Octroie l'autorisation de transmettre une clé publique SSH à l'instance EC2 spécifiée qui sera utilisée pour un SSH de console série.	Écrire	instance*		

Types de ressources définis par Amazon EC2 Instance Connect

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}
instance-connect-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

Clés de condition pour Amazon EC2 Instance Connect

Amazon EC2 Instance Connect définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
ec2-instance-connect:maxTunnelDuration	Filtre l'accès en fonction de la durée de session maximale associée à l'instance	Numérique

Clés de condition	Description	Type
ec2-instance-connect:privateIpAddress	Filtre l'accès en fonction de l'adresse IP privée associée à l'instance	IPAddress
ec2-instance-connect:remotePort	Filtre l'accès en fonction du numéro de port associé à l'instance	Numérique
ec2:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
ec2:osuser	Filtre les accès en spécifiant le nom d'utilisateur par défaut pour l'AMI que vous avez utilisée pour lancer votre instance.	String

Actions, ressources et clés de condition pour le service Amazon ECS MCP

Le service Amazon ECS MCP (préfixe de service :`ecs-mcp`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service Amazon ECS MCP
- Types de ressources définis par le service Amazon ECS MCP
- Clés de condition pour le service Amazon ECS MCP

Actions définies par le service Amazon ECS MCP

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvokeReadOnlyTools	Accorde l'autorisation d'appeler des outils en lecture seule dans le service MCP	Lecture			
UseMcp	Autorise l'utilisation du service MCP	Lecture			

Types de ressources définis par le service Amazon ECS MCP

Le service Amazon ECS MCP ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au service Amazon ECS MCP, spécifiez-le `"Resource": "*"` dans votre politique.

Clés de condition pour le service Amazon ECS MCP

ECS MCP ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon EKS Auth

Amazon EKS Auth (préfixe de service : `eks-auth`) fournit les ressources, actions et clés de contexte de condition propres au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EKS Auth
- Types de ressources définis par Amazon EKS Auth
- Clés de condition pour Amazon EKS Auth

Actions définies par Amazon EKS Auth

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssumeRoleForPodIdentity	Autorise l'échange d'un jeton de compte de service Kubernetes contre des informations d'identification temporaires AWS	Lecture	cluster*		

Types de ressources définis par Amazon EKS Auth

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon EKS Auth

Amazon EKS Auth définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction d'une paire de clé et de valeur d'identification	String

Actions, ressources et clés de condition pour le serveur Amazon EKS MCP

Le serveur Amazon EKS MCP (préfixe de service :`eks-mcp`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le serveur Amazon EKS MCP
- Types de ressources définis par le serveur Amazon EKS MCP
- Clés de condition pour le serveur Amazon EKS MCP

Actions définies par le serveur Amazon EKS MCP

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CallPrivilegedTool	Accorde l'autorisation d'appeler des outils privilégiés dans le service MCP	Écrire			
CallReadOnlyTool	Accorde l'autorisation d'appeler des outils en lecture seule dans le service MCP	Lecture			
InvokeMcp	Autorise l'utilisation du service MCP	Lecture			

Types de ressources définis par le serveur Amazon EKS MCP

Le serveur Amazon EKS MCP ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au serveur Amazon EKS MCP, spécifiez-le `"Resource": "*"` dans votre politique.

Clés de condition pour le serveur Amazon EKS MCP

EKS MCP ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Elastic Beanstalk

AWS Elastic Beanstalk (`elasticbeanstalk`préfixe de service :) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elastic Beanstalk
- Types de ressources définis par AWS Elastic Beanstalk
- Clés de condition pour AWS Elastic Beanstalk

Actions définies par AWS Elastic Beanstalk

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AbortEnvironmentUpdate	Accorde l'autorisation d'annuler la mise à jour de la configuration d'environnement en cours ou le déploiement d'une version de l'application	Écrire	environment*	elasticbeanstalk:InApplication	
AddTags	Accorde l'autorisation d'ajouter des balises à une ressource Elastic Beanstalk et de mettre à jour les valeurs de balise	Identification	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ApplyEnvironmentManagedAction	Accorde l'autorisation d'appliquer immédiatement une action gérée planifiée	Écrire	environment*	elasticbeanstalk:InApplication	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateEnvironmentOperationsRole	Accorde l'autorisation d'associer un rôle d'opérations à un environnement	Écrire	environment*		
CheckDNSAvailability	Accorde l'autorisation de vérifier la disponibilité d'un CNAME	Lecture			
ComposeEnvironments	Accorde l'autorisation de créer ou de mettre à jour un groupe d'environnements, chacun exécutant un composant distinct d'une application spécifique	Écrire	application*		
			applicationversion*	elasticbeanstalk:InApplication	
CreateApplication	Accorde l'autorisation de créer une application	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationVersion	Accorde l'autorisation de créer une version pour une application	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			applicationversion*	elasticbeanstalk:InApplication aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationTemplate	Accorde l'autorisation de créer un modèle de configuration	Écrire	configurationtemplate*	elasticbeanstalk:InApplication	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Accorde l'autorisation de lancer un environnement pour une application	Écrire	environment*	elasticbeanstalk:InApplication	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlatformVersion	Accorde l'autorisation de créer une version pour une plateforme personnalisée	Écrire	platform*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageLocation	Accorde l'autorisation de créer l'emplacement de stockage Amazon S3 pour le compte	Écrire			
DeleteApplication	Accorde l'autorisation de supprimer une application, ainsi que toutes les versions et configurations associées	Écrire	application*		
DeleteApplicationVersion	Accorde l'autorisation de supprimer une version d'une application	Écrire	applicationversion*	elasticbeanstalk:InApplication	
DeleteConfigurationTemplate	Accorde l'autorisation de supprimer un modèle de configuration	Écrire	configurationtemplate*	elasticbeanstalk:InApplication	
DeleteEnvironmentConfiguration	Accorde l'autorisation de supprimer le projet de configuration associé à l'environnement en cours d'exécution	Écrire	environment*	elasticbeanstalk:InApplication	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePlatformVersion	Accorde l'autorisation de supprimer une version d'une plateforme personnalisée	Écrire	platform*		
DescribeAccountAttributes	Accorde l'autorisation de récupérer la liste des attributs de compte, y compris les quotas de ressources	Lecture			
DescribeApplicationVersions	Accorde l'autorisation de récupérer une liste des versions d'applications stockées dans un bucket de stockage AWS Elastic Beanstalk	List	applicationversion	elasticbeanstalk:InApplication	
DescribeApplications	Accorde l'autorisation de récupérer les descriptions des applications existantes	List	application		
DescribeConfigurationOptions	Accorde l'autorisation de récupérer les descriptions des options de configuration de l'environnement	Lecture	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
			solutionstack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeConfigurationSettings	Accorde l'autorisation de récupérer la description des paramètres d'un jeu de configurations	Lecture	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeEnvironmentHealth	Accorde l'autorisation de récupérer des informations sur l'état général d'un environnement	Lecture	environment		
DescribeEnvironmentManagedActionHistory	Accorde l'autorisation de récupérer la liste des actions gérées terminées et ayant échoué d'un environnement	Lecture	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentManagedActions	Accorde l'autorisation de récupérer la liste des actions gérées en cours et à venir d'un environnement	Lecture	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentResources	Accorde l'autorisation de récupérer une liste de AWS ressources pour un environnement	Lecture	environment	elasticbeanstalk:InApplication	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEnvironments	Accorde l'autorisation de récupérer les descriptions des environnements existants	List	environment	elasticbeanstalk:InApplication	
DescribeEvents	Accorde l'autorisation de récupérer la liste des descriptions d'événements correspondant à un ensemble de critères	Lecture	application		
			applicationversion	elasticbeanstalk:InApplication	
			configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeInstancesHealth	Accorde l'autorisation de récupérer des informations plus détaillées sur l'état des instances de l'environnement	Lecture	environment		
DescribePlatformVersion	Accorde l'autorisation de récupérer la description d'une version de plateforme gérée.	Lecture	platform		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateEnvironmentOperationsRole	Accorde l'autorisation de dissocier un rôle d'opérations avec un environnement	Écrire	environment*		
ListAvailableSolutionStacks	Accorde l'autorisation de récupérer la liste des noms de piles de solutions disponibles	List	solutionstack		
ListPlatformBranches	Accorde l'autorisation de récupérer une liste des branches des plateformes disponibles	List			
ListPlatformVersions	Accorde l'autorisation de récupérer la liste des plateformes disponibles	List	platform		
ListTagsForResource	Accorde l'autorisation de récupérer la liste des balises d'une ressource Elastic Beanstalk	Lecture	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutInstanceStatistics	Accorde l'autorisation d'envoyer des statistiques d'instance pour améliorer l'état	Écrire	application*		
			environment*		
RebuildEnvironment	Accorde l'autorisation de supprimer et de recréer toutes les AWS ressources d'un environnement et de forcer le redémarrage	Écrire	environment*	elasticbeanstalk:InApplication	
RemoveTags	Accorde l'autorisation de supprimer les balises d'une ressource Elastic Beanstalk	Identification	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RequestEnvironmentInfo	Accorde l'autorisation d'initier une demande visant à compiler les informations de l'environnement déployé	Lecture	environment*	elasticbeanstalk:InApplication	
RestartAppServer	Accorde l'autorisation de demander à un environnement de redémarrer le serveur conteneur d'application exécuté sur chaque instance Amazon EC2	Écrire	environment*	elasticbeanstalk:InApplication	
RetrieveEnvironmentInfo	Accorde l'autorisation de récupérer les informations compilées à partir d'une RequestEnvironmentInfo demande	Lecture	environment*	elasticbeanstalk:InApplication	
SwapEnvironmentCNAMEs	Autorise l'échange CNAMEs de deux environnements	Écrire	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromEnvironment	
TerminateEnvironment	Accorde l'autorisation de résilier un environnement	Écrire	environment*	elasticbeanstalk:InApplication	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApplication	Accorde l'autorisation de mettre à jour une application avec les propriétés spécifiées	Écrire	application*		
UpdateApplicationResourceLifecycle	Accorde l'autorisation de mettre à jour la politique de cycle de vie de version d'application associée à l'application	Écrire	application*		
UpdateApplicationVersion	Accorde l'autorisation de mettre à jour une version d'application avec les propriétés spécifiées	Écrire	applicationversion*	elasticbeanstalk:InApplication	
UpdateConfigurationTemplate	Accorde l'autorisation de mettre à jour un modèle de configuration avec les propriétés ou les valeurs d'option de configuration spécifiées	Écrire	configurationtemplate*	elasticbeanstalk:InApplication	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEnvironment	Accorde l'autorisation de mettre à jour un environnement	Écrire	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTagsForResource	N'autorise pas la mise à jour des balises. Pour autoriser l'ajout de balises à une ressource Elastic Beanstalk , la suppression de balises et la mise à jour des valeurs des balises, spécifiez elasticbeanstalk : et elasticbeanstalk : AddTags RemoveTags	Identification	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ValidateConfigurationSettings	Accorde l'autorisation de vérifier la validité d'un ensemble de paramètres de configuration pour un modèle de configuration ou un environnement	Lecture	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

Types de ressources définis par AWS Elastic Beanstalk

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}
applicationversion	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:applicationversion/${ApplicationName}/${VersionLabel}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
configurationtemplate	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:configurationtemplate/${ApplicationName}/${TemplateName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
environment	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:environment/${ApplicationName}/${EnvironmentName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
solutionstack	`arn:${Partition}:elasticbeanstalk:${Region}::solutionstack/${SolutionStackName}`	

Types de ressources	ARN	Clés de condition
platform	`arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}`	

Clés de condition pour AWS Elastic Beanstalk

AWS Elastic Beanstalk définit les clés de condition suivantes qui peuvent être utilisées `Condition` dans l'élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString
elasticbeanstalk:FromApplication	Filtre l'accès en fonction d'une application en tant que dépendance ou contrainte dans un paramètre d'entrée	ARN
elasticbeanstalk:FromApplicationVersion	Filtre l'accès en fonction d'une version d'application en tant que dépendance ou contrainte dans un paramètre d'entrée	ARN

Clés de condition	Description	Type
elasticbeanstalk:FromConfigurationTemplate	Filtre l'accès en fonction d'un modèle de configuration en tant que dépendance ou contrainte dans un paramètre d'entrée	ARN
elasticbeanstalk:FromEnvironment	Filtre l'accès en fonction d'un environnement en tant que dépendance ou contrainte dans un paramètre d'entrée	ARN
elasticbeanstalk:FromPlatform	Filtre l'accès en fonction d'une plateforme en tant que dépendance ou contrainte dans un paramètre d'entrée	ARN
elasticbeanstalk:FromSolutionStack	Filtre l'accès en fonction d'une pile de solutions en tant que dépendance ou contrainte dans un paramètre d'entrée	ARN
elasticbeanstalk:InApplication	Filtre l'accès en fonction de l'application qui contient la ressource sur laquelle l'action agit	ARN

Actions, ressources et clés de condition pour Amazon Elastic Block Store

Amazon Elastic Block Store (préfixe de service : `ebs`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic Block Store
- Types de ressources définis par Amazon Elastic Block Store
- Clés de condition pour Amazon Elastic Block Store

Actions définies par Amazon Elastic Block Store

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CompleteSnapshot	Accorde l'autorisation de sceller et de terminer l'instantané après l'écriture de tous les blocs de données requis	Écrire	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	Accorde l'autorisation de renvoyer les données d'un bloc dans un instantané Amazon Elastic Block Store (EBS)	Lecture	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	Autorise à répertorier les blocs différents entre deux instantanés Amazon Elastic Block Store (EBS) de la même lignée volume/snapshot	Lecture	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks	Accorde l'autorisation de répertorier les blocs dans un	Lecture	snapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	instantané Amazon Elastic Block Store (EBS)			aws:ResourceTag/${TagKey}	
PutSnapshotBlock	Accorde l'autorisation d'écrire un bloc de données dans un instantané créé par l'StartSnapshot opération	Écrire	snapshot*		
				aws:ResourceTag/${TagKey}	
StartSnapshot	Accorde l'autorisation de créer un instantané EBS	Écrire	snapshot		ec2:CreateTags
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Types de ressources définis par Amazon Elastic Block Store

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Clés de condition pour Amazon Elastic Block Store

Amazon Elastic Block Store définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
ebs:Description	Filtre l'accès en fonction de la description de l'instantané en cours de création	String
ebs:ParentSnapshot	Filtre l'accès en fonction de l'ARN de l'instantané parent.	ARN
ebs:VolumeSize	Filtre l'accès en fonction de la taille du volume de l'instantané en cours de création, en Gio	Numérique

Actions, ressources et clés de condition pour Amazon Elastic Container Registry

Amazon Elastic Container Registry (préfixe de service : `ecr`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic Container Registry

- Types de ressources définis par Amazon Elastic Container Registry
- Clés de condition pour Amazon Elastic Container Registry

Actions définies par Amazon Elastic Container Registry

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchCheckLayerAvailability	Accorde l'autorisation de vérifier la disponibilité de plusieurs couches d'images dans un registre et un référentiel spécifiés.	Lecture	repository*		
BatchDeleteImage	Accorde l'autorisation de supprimer une liste d'images spécifiées au sein d'un référentiel spécifié.	Écriture	repository*		
BatchGetImage	Accorde l'autorisation d'obtenir des informations détaillées pour les images spécifiées dans un référentiel spécifié	Lecture	repository*		
BatchGetRepositoryScanningConfiguration	Accorde l'autorisation de récupérer la configuration d'analyse du référentiel pour une liste de référentiels	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchImportUpstreamImage [autorisation uniquement]	Accorde l'autorisation de récupérer l'image dans le registre amont et de l'importer dans votre registre privé	Écrire	repository*		
CompleteLayerUpload	Accorde l'autorisation d'informer Amazon ECR que le chargement d'une couche d'image pour le registre, du nom de référentiel et de l'ID de chargement spécifiés est terminé.	Écrire	repository*		
CreatePullThroughCacheRule	Accorde l'autorisation de créer une règle de cache de passage	Écrire			iam:CreateServiceLinkedRole
CreateRepository	Accorde l'autorisation de créer un référentiel d'images.	Écrire	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRepositoryCreationTemplate	Octroie l'autorisation de créer un modèle de création de référentiel.	Écrire			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
DeleteLifecyclePolicy	Accorde l'autorisation de supprimer la politique de cycle de vie spécifiée	Écrire	repository*		
DeletePullThroughCacheRule	Accorde l'autorisation de supprimer la règle de cache de passage	Écrire			
DeleteRegistryPolicy	Accorde l'autorisation de supprimer la politique de registre.	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRepository	Accorde l'autorisation de supprimer un référentiel d'images existant	Écrire	repository*		
DeleteRepositoryCreationTemplate	Octroie l'autorisation de supprimer le modèle de création de référentiel.	Écrire			
DeleteRepositoryPolicy	Accorde l'autorisation de supprimer la politique de référentiel d'un référentiel spécifié	Gestion des autorisations	repository*		
DeleteSigningConfiguration	Accorde l'autorisation de supprimer la configuration de signature pour le registre	Écrire			
DeregisterPullTimeUpdateExclusion	Accorde l'autorisation de désenregistrer une exclusion liée à une mise à jour au moment du pull	Écrire			
DescribeImageReplicationStatus	Autorise la récupération du statut de réplication d'une image dans un registre, y compris, en cas d'échec de la réplication, la raison de cet échec	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeImageScanFindings	Accorde l'autorisation de décrire les résultats de numérisation d'image pour l'image spécifiée	Lecture	repository*		
DescribeImageSigningStatus	Accorde l'autorisation de récupérer le statut de signature d'une image dans un registre spécifié	Lecture	repository*		
DescribeImages	Accorde l'autorisation de récupérer les métadonnées sur les images dans un référentiel, y compris la taille de l'image, les balises de l'image et la date de création.	List	repository*		
DescribePullThroughCacheRules	Accorde l'autorisation de décrire les règles de cache de passage	List			
DescribeRegistry	Accorde l'autorisation de décrire les paramètres du registre.	Lecture			
DescribeRepositories	Accorde l'autorisation de décrire des référentiels d'images dans un registre	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRepositoryCreationTemplates	Octroie l'autorisation de décrire le modèle de création de référentiel.	Lecture			
GetAccountSetting	Accorde l'autorisation de récupérer les paramètres du compte	Lecture		ecr:AccountSetting	
GetAuthorizationToken	Accorde l'autorisation de récupérer un jeton valide pour un registre spécifié pendant 12 heures	Lecture			
GetDownloadUrlForLayer	Accorde l'autorisation de récupérer l'URL de téléchargement correspondant à une couche d'image	Lecture	repository*		
GetImageCopyStatus [autorisation uniquement]	Accorde l'autorisation de récupérer le statut d'une copie d'image	Lecture	repository*		
GetLifecyclePolicy	Accorde l'autorisation de récupérer la politique de cycle de vie spécifiée	Lecture	repository*		
GetLifecyclePolicyPreview	Accorde l'autorisation de récupérer les résultats de la demande d'aperçu de politique de cycle de vie spécifiée	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRegistryPolicy	Accorde l'autorisation de récupérer la politique de registre.	Lecture			
GetRegistryScanningConfiguration	Accorde l'autorisation de récupérer une configuration de numérisation de registre	Lecture			
GetRepositoryPolicy	Accorde l'autorisation de récupérer la politique de référentiel pour un référentiel spécifié	Lecture	repository*		
GetSigningConfiguration	Accorde l'autorisation de récupérer la configuration de signature pour le registre	Lecture			
InitiateLayerUpload	Accorde l'autorisation de notifier Amazon ECR que vous avez l'intention de charger une couche d'image	Écrire	repository*		
ListImages	Accorde l'autorisation de répertorier toutes les images IDs d'un référentiel donné	List	repository*		
ListPullTimeUpdateExclusions	Octroie l'autorisation de répertorier les exclusions de mise à jour au moment du retrait pour le registre	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour une ressource Amazon ECR	Lecture	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutAccountSetting	Accorde l'autorisation de mettre à jour les paramètres du compte	Écrire		ecr:AccountSetting	
PutImage	Accorde l'autorisation de créer ou de mettre à jour le manifeste d'image associé à une image	Écriture	repository*		
PutImageScanningConfiguration	Accorde l'autorisation de mettre à jour la configuration de numérisation d'images pour un référentiel	Écriture	repository*		
PutImageTagMutability	Accorde l'autorisation de mettre à jour les paramètres d'immuabilité des balises d'image pour un référentiel	Écriture	repository*		
PutLifecyclePolicy	Accorde l'autorisation de créer ou de mettre à jour une politique de cycle de vie	Écriture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutRegistryPolicy	Accorde l'autorisation de mettre à jour la politique de registre.	Gestion des autorisations			
PutRegistryScanningConfiguration	Accorde l'autorisation de mettre à jour la configuration de numérisation de registre	Écrire			
PutReplicationConfiguration	Accorde l'autorisation de mettre à jour la configuration de la réplication pour le registre.	Écrire			iam:CreateServiceLinkedRole
PutSigningConfiguration	Accorde l'autorisation de mettre à jour la configuration de signature pour le registre	Écrire			
RegisterPullTimeUpdateExclusion	Autorise l'enregistrement d'une exclusion liée à la mise à jour au moment du téléchargement	Écrire			
ReplicateImage [autorisation uniquement]	Accorde l'autorisation de répliquer des images vers le registre de destination.	Écriture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetRepositoryPolicy	Accorde l'autorisation d'appliquer une politique de référentiel sur un référentiel spécifié pour contrôler les autorisations d'accès	Gestion des autorisations	repository*		
StartImageScan	Accorde l'autorisation de démarrer une numérisation d'image	Écriture	repository*		
StartLifecyclePolicyPreview	Accorde l'autorisation de démarrer un aperçu de la politique de cycle de vie spécifiée	Écriture	repository*		
TagResource	Accorde l'autorisation de baliser une ressource Amazon ECR	Balisage	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource Amazon ECR	Identification	repository*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateImageStorageClass	Accorde l'autorisation de mettre à jour la classe de stockage d'une image spécifiée dans un référentiel spécifié	Écrire	repository*		
UpdatePullThroughCacheRule	Octroie l'autorisation de mettre à jour la règle de cache de passage.	Écrire			
UpdateRepositoryCreationTemplate	Accorde l'autorisation de mettre à jour le modèle de création de référentiel	Écrire			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
UploadLayerPart	Accorde l'autorisation de charger une partie de couche d'image dans Amazon ECR	Écrire	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ValidatePullThroughCacheRule	Octroie l'autorisation de valider la règle de cache de passage.	Lecture			

Types de ressources définis par Amazon Elastic Container Registry

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
repository	`arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr:ResourceTag/${TagKey}

Clés de condition pour Amazon Elastic Container Registry

Amazon Elastic Container Registry définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString
ecr:AccountSetting	Filtre l'accès en fonction du nom du paramètre du compte ECR	String
ecr:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String

Actions, ressources et clés de condition pour Amazon Elastic Container Registry Public

Amazon Elastic Container Registry Public (préfixe de service : `ecr-public`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic Container Registry Public
- Types de ressources définis par Amazon Elastic Container Registry Public
- Clés de condition pour Amazon Elastic Container Registry Public

Actions définies par Amazon Elastic Container Registry Public

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchCheckLayerAvailability	Accorde l'autorisation de vérifier la disponibilité de plusieurs couches d'images dans un registre et un référentiel spécifiés.	Lecture	repository*		
BatchDeleteImage	Accorde l'autorisation de supprimer une liste d'images spécifiées au sein d'un référentiel spécifié.	Écriture	repository*		
CompleteLayerUpload	Accorde l'autorisation d'informer Amazon ECR que le chargement d'une couche d'image pour le registre, du nom de référentiel et de l'ID de chargement spécifiés est terminé.	Écriture	repository*		
CreateRepository	Accorde l'autorisation de créer un référentiel d'images.	Écriture	repository*		ecr-public:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRepository	Accorde l'autorisation de supprimer un référentiel d'images existant	Écriture	repository*		
DeleteRepositoryPolicy	Accorde l'autorisation de supprimer la politique de référentiel d'un référentiel spécifié	Écriture	repository*		
DescribeImageTags	Accorde l'autorisation de décrire toutes les balises d'image pour un référentiel donné.	Liste	repository*		
DescribeImages	Accorde l'autorisation de récupérer les métadonnées sur les images dans un référentiel, y compris la taille de l'image, les balises de l'image et la date de création.	Lecture	repository*		
DescribeRegistries	Accorde l'autorisation de récupérer les données de catalogue associées à un registre.	Liste	registry*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRepositories	Accorde l'autorisation de décrire des référentiels d'images dans un registre	Liste	repository		
GetAuthorizationToken	Accorde l'autorisation de récupérer un jeton valide pour un registre spécifié pendant 12 heures	Lecture			
GetRegistryCatalogData	Accorde l'autorisation de récupérer les données de catalogue associées à un registre.	Lecture	registry*		
GetRepositoryCatalogData	Accorde l'autorisation de récupérer les données de catalogue associées à un référentiel.	Lecture	repository*		
GetRepositoryPolicy	Accorde l'autorisation de récupérer la politique de référentiel pour un référentiel spécifié	Lecture	repository*		
InitiateLayerUpload	Accorde l'autorisation de notifier Amazon ECR que vous avez l'intention de charger une couche d'image	Écriture	repository*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour une ressource Amazon ECR	Lecture	repository*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutImage	Accorde l'autorisation de créer ou de mettre à jour le manifeste d'image associé à une image	Écriture	repository*		
PutRegistryCatalogData	Accorde l'autorisation de créer et de mettre à jour les données de catalogue associées à un registre.	Écriture	registry*		
PutRepositoryCatalogData	Accorde l'autorisation de mettre à jour les données de catalogue associées à un référentiel.	Écriture	repository*		
SetRepositoryPolicy	Accorde l'autorisation d'appliquer une politique de référentiel sur un référentiel spécifié pour contrôler les autorisations d'accès	Gestion des autorisations	repository*		
TagResource	Accorde l'autorisation de baliser une ressource Amazon ECR	Balisage	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource Amazon ECR	Balisage	repository*		
				aws:TagKeys	
UploadLayerPart	Accorde l'autorisation de charger une partie de couche d'image sur Amazon ECR Public	Écriture	repository*		

Types de ressources définis par Amazon Elastic Container Registry Public

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
repository	`arn:${Partition}:ecr-public::${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr-public:ResourceTag/${TagKey}
registry	`arn:${Partition}:ecr-public::${Account}:registry/${RegistryId}`	

Clés de condition pour Amazon Elastic Container Registry Public

Amazon Elastic Container Registry Public définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les demandes de création en fonction de l'ensemble de valeurs autorisées pour chacune des balises.	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur de balise associée à la ressource.	Chaîne
aws:TagKeys	Filtre les demandes de création en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString
ecr-public:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur de balise associée à la ressource.	Chaîne

Actions, ressources et clés de condition pour AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery (préfixe de service :`drs`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elastic Disaster Recovery
- Types de ressources définis par AWS Elastic Disaster Recovery
- Clés de condition pour AWS Elastic Disaster Recovery

Actions définies par AWS Elastic Disaster Recovery

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateFailbackClientToRecoveryInstanceForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir le client de failback associé vers une instance de récupération	Écrire	RecoveryInstanceResource*		
AssociateSourceNetworkStack	Accorde l'autorisation d'associer une CloudFormation pile au réseau source	Écrire	SourceNetworkResource*		cloudformation:DescribeStackResource cloudformation:DescribeStacks

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchCreateVolumeSnapshotGroupForDrs [autorisation uniquement]	Accorde l'autorisation de créer un groupe d'instantanés de volume par lots	Écrire	RecoveryInstanceResource*		
			SourceServerResource*		
BatchDeleteSnapshotRequestForDrs [autorisation uniquement]	Accorde l'autorisation de supprimer par lot la demande d'instantané.	Écrire			
CreateConvertedSnapshotForDrs [autorisation uniquement]	Accorde l'autorisation de créer un instantané converti	Écrire	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExtendedSourceServer	Accorde l'autorisation d'étendre un serveur source	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	drs:DescribeSourceServers drs:GetReplicationConfiguration
CreateLaunchConfigurationTemplate	Accorde l'autorisation de créer un modèle de configuration du lancement	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryInstanceForDrs [autorisation uniquement]	Accorde l'autorisation de créer une instance de récupération	Écrire	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReplicationConfigurationTemplate	Accorde l'autorisation de créer un modèle de configuration de réplication.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey
CreateSourceNetwork	Accorde l'autorisation de créer un réseau source	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSourceServerForDrs [autorisation uniquement]	Accorde l'autorisation de créer un serveur source	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJob	Accorde l'autorisation de supprimer une tâche.	Écrire	JobResource*		
DeleteLaunchAction	Accorde l'autorisation de supprimer une action de lancement	Écrire	LaunchConfigurationTemplateResource		
			SourceServerResource		
DeleteLaunchConfigurationTemplate	Accorde l'autorisation de supprimer le modèle de configuration du lancement	Écrire	LaunchConfigurationTemplateResource*		
DeleteRecoveryInstance	Accorde l'autorisation de supprimer une instance de récupération	Écrire	RecoveryInstanceResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteReplicationConfigurationTemplate	Accorde l'autorisation de supprimer un modèle de configuration de réplication.	Écrire	ReplicationConfigurationTemplateResource*		
DeleteSourceNetwork	Accorde l'autorisation de supprimer un réseau source	Écrire	SourceNetworkResource*		
DeleteSourceServer	Accorde l'autorisation de supprimer le serveur source.	Écriture	SourceServerResource*		
DescribeJobLogItems	Accorde l'autorisation de décrire les éléments du journal des tâches.	Lecture	JobResource*		
DescribeJobs	Accorde l'autorisation de décrire les tâches.	Lecture			
DescribeLaunchConfigurationTemplates	Accorde l'autorisation de décrire le modèle de configuration du lancement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRecoveryInstances	Accorde l'autorisation de décrire les instances de récupération	Lecture			drs:DescribeSourceServers ec2:DescribeInstances
DescribeRecoverySnapshots	Accorde l'autorisation de décrire les instantanés de récupération	Lecture	SourceServerResource*		
DescribeReplicationConfigurationTemplates	Accorde l'autorisation de décrire le modèle de configuration de réplication.	Lecture			
DescribeReplicationServerAssociationsForDrs [autorisation uniquement]	Accorde l'autorisation de décrire les associations de serveur de réplication.	Lecture			
DescribeSnapshotRequestsForDrs [autorisation uniquement]	Accorde l'autorisation de décrire les demandes d'instantanés.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSourceNetworks	Accorde l'autorisation de décrire les réseaux source	Lecture			
DescribeSourceServers	Accorde l'autorisation de décrire les serveurs source.	Lecture			
DisconnectRecoveryInstance	Accorde l'autorisation de déconnecter l'instance de récupération	Écrire	RecoveryInstanceResource*		
DisconnectSourceServer	Accorde l'autorisation de déconnecter le serveur source	Écrire	SourceServerResource*		
ExportSourceNetworkCfnTemplate	Autorise l'exportation d' CloudFormation un modèle contenant des ressources du réseau source	Écrire	SourceNetworkResource*		s3:GetBucketLocation s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAgentCommandForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir la commande de l'agent.	Lecture	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentConfirmedResumeInfoForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations de reprise confirmées par l'agent.	Lecture	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentInstallationAssetsForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir les ressources d'installation de l'agent.	Lecture			
GetAgentReplicationInfoForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations de réplication de l'agent.	Lecture	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAgentRuntimeConfigurationForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir la configuration d'exécution de l'agent.	Lecture	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentSnapshotCreditsForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir des crédits d'instantanés de l'agent.	Lecture	RecoveryInstanceResource*		
			SourceServerResource*		
GetChannelCommandsForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir des commandes de canal.	Lecture			
GetFailbackCommandForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir la commande de failback	Lecture	RecoveryInstanceResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFailbackLaunchRequestedForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir le lancement du failback demandé	Lecture	RecoveryInstanceResource*		
GetFailbackReplicationConfiguration	Accorde l'autorisation d'obtenir la configuration de réplication du failback	Lecture	RecoveryInstanceResource*		
GetLaunchConfiguration	Accorde l'autorisation d'obtenir la configuration de lancement.	Lecture	SourceServerResource*		
GetReplicationConfiguration	Accorde l'autorisation d'obtenir la configuration de réplication.	Lecture	SourceServerResource*		
GetSuggestedFailbackClientDeviceMappingForDrs [autorisation uniquement]	Accorde l'autorisation d'obtenir le mappage de l'appareil client du failback suggéré	Lecture	RecoveryInstanceResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InitializeService	Accorde l'autorisation d'initialiser le service.	Écrire			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueAgentCertificateForDrs [autorisation uniquement]	Accorde l'autorisation d'émettre un certificat d'agent	Écrire	RecoveryInstanceResource* SourceServerResource*		
ListExtensibleSourceServers	Accorde l'autorisation de répertorier les serveurs source extensibles	Lecture			drs:DescribeSourceServers

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLaunchActions	Accorde l'autorisation de répertorier les actions de lancement	Lecture	LaunchConfigurationTemplateResource		
			SourceServerResource		
ListStagingAccounts	Accorde l'autorisation de répertorier les comptes de mise en attente	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture			
NotifyAgentAuthenticationForDrs [autorisation uniquement]	Accorde l'autorisation de signaler l'authentification de l'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentConnectedForDrs [autorisation uniquement]	Accorde l'autorisation de signaler que l'agent est connecté.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
NotifyAgentDisconnectedForDrs [autorisation uniquement]	Accorde l'autorisation de signaler que l'agent est déconnecté.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentReplicationProgressForDrs [autorisation uniquement]	Accorde l'autorisation de signaler la progression de la réplication de l'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyConsistencyAttainedForDrs [autorisation uniquement]	Accorde l'autorisation de signaler que la cohérence est atteinte	Écrire	RecoveryInstanceResource*		
NotifyReplicationServerAuthenticationForDrs [autorisation uniquement]	Accorde l'autorisation de signaler l'authentification du serveur de réplication	Écrire	RecoveryInstanceResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
NotifyVolumeEventForDrs [autorisation uniquement]	Accorde l'autorisation de signaler des événements de volume de réplication	Écrire	SourceServerResource*		
PutLaunchAction	Accorde l'autorisation de placer une action de lancement	Écrire	LaunchConfigurationTemplateResource		ssm:DescribeDocument
			SourceServerResource		
RetryDataReplication	Accorde l'autorisation de réessayer la réplication des données.	Écrire	SourceServerResource*		
ReverseReplication	Accorde l'autorisation d'inverser la réplication	Écrire	RecoveryInstanceResource*		drs:DescribeReplicationConfigurationTemplates drs:DescribeSourceServers ec2:DescribeInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
SendAgentLogsForDrs [autorisation uniquement]	Accorde l'autorisation d'envoyer des journaux d'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
SendAgentMetricsForDrs [autorisation uniquement]	Accorde l'autorisation d'envoyer des métriques d'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
SendChannelCommandResultForDrs [autorisation uniquement]	Accorde l'autorisation d'envoyer le résultat de la commande de canal.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendClientLogsForDrs [autorisation uniquement]	Accorde l'autorisation d'envoyer des journaux client.	Écriture			
SendClientMetricsForDrs [autorisation uniquement]	Accorde l'autorisation d'envoyer des métriques client.	Écrire			
SendVolumeStatsForDrs [autorisation uniquement]	Accorde l'autorisation d'envoyer des statistiques sur le débit du volume	Écrire	SourceServerResource*		
StartFailbackLaunch	Accorde l'autorisation de démarrer le lancement du failback	Écrire	RecoveryInstanceResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartRecovery	Accorde l'autorisation de démarrer la récupération	Écrire	SourceServerResource*		drs:CreateRecoveryInstanceForDrs drs:ListTagsForResource ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSnapshot

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:CreateTags ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstan

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeSubnets ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:TerminateInstances iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StartReplication	Accorde l'autorisation de démarrer la réplication	Écrire	SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartSourceNetworkRecovery	Accorde l'autorisation de démarrer la récupération du réseau	Écrire	SourceNetworkResource*		cloudformation:CreateStack cloudformation:DescribeStackResource cloudformation:DescribeStacks cloudformation:UpdateStack drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartSourceNetworkReplication	Accorde l'autorisation de démarrer la réplication du réseau	Écrire	SourceNetworkResource*		
StopFailback	Accorde l'autorisation d'arrêter le failback	Écrire	RecoveryInstanceResource*		
StopReplication	Accorde l'autorisation d'arrêter la réplication	Écrire	SourceServerResource*		
StopSourceNetworkReplication	Accorde l'autorisation d'arrêter la réplication du réseau	Écrire	SourceNetworkResource*		
TagResource	Accorde l'autorisation d'attribuer une balise de ressource.	Identification	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		
				aws:RequestTag/${TagKey} aws:TagKeys drs:CreateAction	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TerminateRecoveryInstances	Accorde l'autorisation de terminer les instances de récupération	Écrire	RecoveryInstanceResource*		drs:DescribeSourceServers ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	JobResource		
			LaunchConfigurationTemplateResource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		
				aws:TagKeys	
UpdateAgentBacklogForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour le backlog de l'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgentConversionInfoForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour les informations de conversion de l'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationInfoForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour les informations de réplication de l'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationProcessStateForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour l'état du processus de réplication de l'agent.	Écriture	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentSourcePropertiesForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour les propriétés sources de l'agent.	Écrire	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFailbackClientDeviceMappingForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour le mappage de l'appareil client du failback	Écrire	RecoveryInstanceResource*		
UpdateFailbackClientLastSeenForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour le dernier client du failback vu	Écrire	RecoveryInstanceResource*		
UpdateFailbackReplicationConfiguration	Accorde l'autorisation de mettre à jour la configuration de réplication du failback	Écrire	RecoveryInstanceResource*		
UpdateLaunchConfiguration	Accorde l'autorisation de mettre à jour la configuration de lancement.	Écrire	SourceServerResource*		ec2:DescribeInstances
UpdateLaunchConfigurationTemplate	Accorde l'autorisation de mettre à jour la configuration de lancement.	Écrire	LaunchConfigurationTemplateResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateReplicationCertificateForDrs [autorisation uniquement]	Accorde l'autorisation de mettre à jour un certificat de réplication	Écrire	RecoveryInstanceResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateReplicationConfiguration	Accorde l'autorisation de mettre à jour la configuration de réplication.	Écriture	SourceServerResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateReplicationConfigurationTemplate	Accorde l'autorisation de mettre à jour le modèle de configuration de réplication.	Écrire	ReplicationConfigurationTemplateResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Types de ressources définis par AWS Elastic Disaster Recovery

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
JobResource	`arn:${Partition}:drs:${Region}:${Account}:job/${JobID}`	aws:ResourceTag/${TagKey}
RecoveryInstanceResource	`arn:${Partition}:drs:${Region}:${Account}:recovery-instance/${RecoveryInstanceID}`	aws:ResourceTag/${TagKey} drs:EC2InstanceARN
ReplicationConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
SourceServerResource	`arn:${Partition}:drs:${Region}:${Account}:source-server/${SourceServerID}`	aws:ResourceTag/${TagKey}
SourceNetworkResource	`arn:${Partition}:drs:${Region}:${Account}:source-network/${SourceNetworkID}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
drs:CreateAction	Filtre l'accès en fonction du nom d'une action d'API de création de ressources.	String
drs:EC2InstanceARN	Filtre l'accès en fonction de l'instance EC2 à l'origine de la demande.	ARN

Actions, ressources et clés de condition pour Amazon Elastic File System

Amazon Elastic File System (préfixe de service : `elasticfilesystem`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic File System

- Types de ressources définis par Amazon Elastic File System
- Clés de condition pour Amazon Elastic File System

Actions définies par Amazon Elastic File System

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Backup [autorisation uniquement]	Accorde l'autorisation de lancer une tâche de sauvegarde pour un système de fichiers existant.	Écriture	file-system*		
ClientMount [autorisation uniquement]	Accorde l'autorisation à un client NFS d'accéder en lecture à un système de fichiers.	Lecture	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ClientRootAccess [autorisation uniquement]	Accorde l'autorisation à un client NFS d'accéder en racine à un système de fichiers.	Écriture	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientWrite [autorisation uniquement]	Accorde l'autorisation à un client NFS d'accéder en écriture à un système de fichiers.	Écriture	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
CreateAccessPoint	Accorde l'autorisation de créer un point d'accès pour le système de fichiers spécifié.	Écriture	file-system*		elasticfilesystem:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFileSystem	Accorde l'autorisation de créer un système de fichiers vide.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:Encrypted	elasticfilesystem:TagResource
CreateMountTarget	Accorde l'autorisation de créer une cible de montage pour un système de fichiers.	Écrire	file-system*		
CreateReplicationConfiguration	Accorde l'autorisation de créer une configuration de réplication	Écrire	file-system*		
CreateTags	Accorde l'autorisation de créer ou de remplacer des balises associées à un système de fichiers ; obsolète, voir TagResource	Identification	file-system*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPoint	Accorde l'autorisation de supprimer le point d'accès spécifié.	Écriture	access-point*		
DeleteFileSystem	Accorde l'autorisation de supprimer un système de fichiers en coupant définitivement l'accès à son contenu.	Écriture	file-system*		
DeleteFileSystemPolicy	Accorde l'autorisation de supprimer la politique au niveau des ressources pour un système de fichiers.	Gestion des autorisations	file-system*		
DeleteMountTarget	Accorde l'autorisation de supprimer la cible de montage spécifiée.	Écrire	file-system*		
DeleteReplicationConfiguration	Accorde l'autorisation de supprimer une configuration de réplication	Écrire	file-system*		
DeleteTags	Accorde l'autorisation de supprimer les balises spécifiées d'un système de fichiers ; obsolète, voir UntagResource	Identification	file-system*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DescribeAccessPoints	Accorde l'autorisation d'afficher les descriptions des points d'accès Amazon EFS.	Liste	access-point		
			file-system		
DescribeAccountPreferences	Accorde l'autorisation d'afficher les préférences de compte en vigueur pour un compte	List			
DescribeBackupPolicy	Autorise l'affichage de l'BackupPolicy objet pour un système de fichiers Amazon EFS	Lecture	file-system*		
DescribeFileSystemPolicy	Accorde l'autorisation d'afficher la politique au niveau des ressources pour un système de fichiers Amazon EFS.	Lecture	file-system		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFileSystems	Accorde l'autorisation de consulter la description d'un système de fichiers Amazon EFS spécifié par le système de fichiers FileSystemId ; CreationToken ou de consulter la description de tous les systèmes de fichiers appartenant Compte AWS à l'appelant dans la AWS région du point de terminaison appelé	List	file-system		
DescribeLifecycleConfiguration	Autorise l'affichage de l' LifecycleConfiguration objet pour un système de fichiers Amazon EFS	Lecture	file-system*		
DescribeMountTargetSecurityGroups	Accorde l'autorisation d'afficher les groupes de sécurité en vigueur pour une cible de montage.	Lecture	file-system*		
DescribeMountTargets	Accorde l'autorisation d'afficher les descriptions de toutes les cibles de montage ou d'une cible de montage spécifique pour un système de fichiers.	Lecture	file-system*		
			access-point		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReplicationConfigurations	Accorde l'autorisation de consulter la description d'une configuration de réplication Amazon EFS spécifiée par FileSystemId ; ou de consulter la description de toutes les configurations de réplication détenues par l'appelant Compte AWS dans la AWS région du point de terminaison appelé	List	file-system		
DescribeTags	Accorde l'autorisation d'afficher les balises associées à un système de fichiers.	Lecture	file-system*		
ListTagsForResource	Accorde l'autorisation d'afficher les balises associées à la ressource Amazon EFS spécifiée.	Lecture	access-point		
			file-system		
ModifyMountTargetSecurityGroups	Accorde l'autorisation de modifier l'ensemble des groupes de sécurité en vigueur pour une cible de montage.	Écriture	file-system*		
PutAccountPreferences	Accorde l'autorisation de définir les préférences de compte d'un compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutBackupPolicy	Accorde l'autorisation d'activer ou de désactiver les sauvegardes automatiques avec AWS Backup en créant un nouvel BackupPolicy objet	Écrire	file-system*		
PutFileSystemPolicy	Accorde l'autorisation d'appliquer une politique au niveau des ressources qui définit les actions autorisées ou refusées par des acteurs donnés pour le système de fichiers spécifié.	Gestion des autorisations	file-system*		
PutLifecycleConfiguration	Accorde l'autorisation d'activer la gestion du cycle de vie en créant un nouvel Lifecycle Configuration objet	Écrire	file-system*		
ReplicationRead [autorisation uniquement]	Accorde l'autorisation de lire les données du système de fichiers pour la réplication	Lecture	file-system*		
ReplicationWrite [autorisation uniquement]	Accorde l'autorisation de répliquer des données dans un système de fichiers	Écrire	file-system*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Restore [autorisation uniquement]	Accorde l'autorisation de lancer une tâche de restauration pour une sauvegarde d'un système de fichiers.	Écriture	file-system*		
TagResource	Accorde l'autorisation de créer ou d'écraser les balises associées à la ressource Amazon EFS spécifiée.	Balisage	access-point		
			file-system		
				aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:CreateAction	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées d'une ressource Amazon EFS.	Balisage	access-point		
			file-system		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFileSystem	Accorde l'autorisation de mettre à jour le mode de débit ou la quantité de débit allouée d'un système de fichiers existant.	Écrire	file-system*		
UpdateFileSystemProtection	Octroie l'autorisation de mettre à jour la protection du système de fichiers d'un système de fichiers existant.	Écrire	file-system*		

Types de ressources définis par Amazon Elastic File System

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
file-system	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
access-point	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Elastic File System

Amazon Elastic File System définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
elasticfilesystem:AccessPointArn	Filtre l'accès en fonction de l'ARN du point d'accès utilisé pour monter le système de fichiers.	ARN
elasticfilesystem:AccessedViaMountTarget	Filtre l'accès en fonction de l'accès au système de fichiers via des cibles de montage.	Booléen
elasticfilesystem:CreateAction	Filtre l'accès en fonction du nom d'une action d'API de création de ressources.	String
elasticfilesystem:Encrypted	Filtre l'accès en fonction de la possibilité pour les utilisateurs de créer uniquement des systèmes de fichiers chiffrés ou non chiffrés.	Booléen

Actions, ressources et clés de condition pour Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (préfixe de service : `eks`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic Kubernetes Service
- Types de ressources définis par Amazon Elastic Kubernetes Service
- Clés de condition pour Amazon Elastic Kubernetes Service

Actions définies par Amazon Elastic Kubernetes Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AccessKubernetesApi [autorisation uniquement]	Autorise l'affichage des objets Kubernetes via la console EKS AWS	Lecture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAccessPolicy	Accorde l'autorisation d'associer une stratégie d'accès Amazon EKS à une entrée d'accès Amazon EKS	Écrire	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
AssociateEncryptionConfig	Accorde l'autorisation d'associer la configuration du chiffrement à un cluster	Écriture	cluster*		
AssociateIdentityProviderConfig	Accorde l'autorisation d'associer une configuration de fournisseur d'identité à un cluster	Écrire	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:clientId eks:issuerUrl	
CreateAccessEntry	Accorde l'autorisation de créer une entrée d'accès Amazon EKS	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	Accorde l'autorisation de créer un module complémentaire Amazon EKS	Écrire	cluster*		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCapability	Accorde l'autorisation de créer une fonctionnalité pour un cluster Amazon EKS	Écrire	cluster*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCluster	Accorde l'autorisation de créer un cluster Amazon EKS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions eks:bootstrapSelfManagedAddons eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				eks:blockStorageEnabled eks:loggingType/${type}	
CreateEksAnywhereSubscription	Accorde l'autorisation de mettre à jour un abonnement EKS Anywhere	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	Accorde l'autorisation de créer un profil AWS Fargate	Écrire	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Accorde l'autorisation de créer un groupe de nœuds Amazon EKS	Écrire	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePodIdentityAssociation	Octroie l'autorisation de créer une association d'identité du pod EKS.	Écrire	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	Accorde l'autorisation de supprimer une entrée d'accès Amazon EKS	Écrire	access-entry*		
DeleteAddon	Accorde l'autorisation de supprimer un module complémentaire Amazon EKS	Écrire	addon*		
			podidentityassociation		
DeleteCapability	Accorde l'autorisation de supprimer une fonctionnalité d'un cluster Amazon EKS	Écrire	capability*		
DeleteCluster	Accorde l'autorisation de supprimer un cluster Amazon EKS	Écrire	cluster*		
DeleteEksAnywhereSubscription	Accorde l'autorisation de décrire un abonnement EKS Anywhere	Écrire	eks-anywhere-subscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFargateProfile	Autorise la suppression d'un profil AWS Fargate	Écrire	fargateprofile*		
DeleteNodegroup	Accorde l'autorisation de supprimer un groupe de nœuds Amazon EKS	Écrire	nodegroup*		
DeletePodIdentityAssociation	Octroie l'autorisation de supprimer une association d'identité du pod EKS.	Écrire	podidentityassociation*		
DeregisterCluster	Accorde l'autorisation d'annuler l'enregistrement d'un cluster externe	Écrire	cluster*		
DescribeAccessEntry	Accorde l'autorisation de décrire une entrée d'accès Amazon EKS	Lecture	access-entry*		
DescribeAddon	Accorde l'autorisation de récupérer des informations descriptives sur un module complémentaire Amazon EKS	Lecture	addon*		
DescribeAddonConfiguration	Accorde l'autorisation de répertorier des options de configuration sur un module complémentaire Amazon EKS	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAddonVersions	Accorde l'autorisation de récupérer des informations de version descriptives sur les modules complémentaires pris en charge par les modules complémentaires Amazon EKS	Lecture			
DescribeCapability	Accorde l'autorisation de décrire une fonctionnalité pour un cluster Amazon EKS	Lecture	capability*		
DescribeCluster	Accorde l'autorisation de récupérer des informations descriptives sur un cluster Amazon EKS	Lecture	cluster*		
DescribeClusterVersions	Accorde l'autorisation de récupérer des informations descriptives sur les versions de Kubernetes prises en charge par les clusters Amazon EKS	Lecture			
DescribeEksAnywhereSubscription	Accorde l'autorisation de décrire un abonnement EKS Anywhere	Lecture	eks-anywhere-subscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFargateProfile	Accorde l'autorisation de récupérer des informations descriptives sur un profil AWS Fargate associé à un cluster	Lecture	fargateprofile*		
DescribeIdentityProviderConfig	Accorde l'autorisation de récupérer des informations descriptives sur une configuration Idp associée à un cluster	Lecture	identityproviderconfig*		
DescribeInsight	Accorde l'autorisation de récupérer des informations descriptives sur une information détectée pour un cluster spécifié	Lecture	cluster*		
DescribeInsightsRefresh	Accorde l'autorisation de récupérer l'état de la dernière opération d'actualisation des informations sur le cluster à la demande	Lecture	cluster*		
DescribeNodegroup	Accorde l'autorisation de récupérer des informations descriptives sur un groupe de nœuds Amazon EKS	Lecture	nodegroup*		
DescribePodIdentityAssociation	Octroie l'autorisation de décrire une association d'identité du pod EKS.	Lecture	podidentityassociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeUpdate	Accorde l'autorisation de récupérer une mise à jour donnée pour un Amazon EKS donné cluster/nodegroup/add-on (dans la région spécifiée ou par défaut)	Lecture	cluster*		
			addon		
			capability		
			nodegroup		
DisassociateAccessPolicy	Accorde l'autorisation de dissocier une stratégie d'accès Amazon EKS d'une entrée d'accès Amazon EKS	Écrire	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	
DisassociateIdentityProviderConfig	Accorde l'autorisation de supprimer une configuration Idp associée	Écrire	identityproviderconfig*		
ListAccessEntries	Accorde l'autorisation de répertorier toutes les entrées d'accès Amazon EKS	List	cluster*		
ListAccessPolicies	Accorde l'autorisation de répertorier les stratégies d'accès Amazon EKS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAddons	Accorde l'autorisation de répertorier les modules complémentaires Amazon EKS dans votre région Compte AWS (dans la région spécifiée ou par défaut) pour un cluster donné	List	cluster*		
ListAssociatedAccessPolicies	Accorde l'autorisation de répertorier une stratégie d'accès associée à une entrée d'accès Amazon EKS	List	access-entry*		
ListCapabilities	Accorde l'autorisation de répertorier les fonctionnalités d'un cluster Amazon EKS	List	cluster*		
ListClusters	Accorde l'autorisation de répertorier les clusters Amazon EKS de votre région Compte AWS (dans la région spécifiée ou par défaut)	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDashboardData	Accorde l'autorisation de répertorier les données du tableau de bord. Le tableau de bord Amazon EKS regroupe les informations relatives aux ressources du cluster sur plusieurs comptes et régions. Le tableau de bord inclut des informations sur les instances EC2 et les versions du cluster EKS	Lecture	dashboard*		
ListDashboardResources	Accorde l'autorisation de répertorier les ressources du tableau de bord. Le tableau de bord Amazon EKS regroupe les informations relatives aux ressources du cluster sur plusieurs comptes et régions. Le tableau de bord inclut des informations sur les instances EC2 et les versions du cluster EKS	Lecture	dashboard*		
ListEksAnywhereSubscriptions	Accorde l'autorisation de répertorier les abonnements EKS Anywhere	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFargateProfiles	Accorde l'autorisation de répertorier les AWS profils Fargate dans Compte AWS votre région (dans la région spécifiée ou par défaut) associés à un cluster donné	List	cluster*		
ListIdentityProviderConfigs	Accorde l'autorisation de répertorier les configurations Idp dans votre Compte AWS (dans la région spécifiée ou par défaut) associées à un cluster donné	List	cluster*		
ListInsights	Accorder l'autorisation de répertorier toutes les informations détectées pour un cluster spécifié	List	cluster*		
ListNodegroups	Accorde l'autorisation de répertorier les groupes de nœuds Amazon EKS de votre région Compte AWS (dans la région spécifiée ou par défaut) rattachés à un cluster donné	List	cluster*		
ListPodIdentityAssociations	Octroie l'autorisation de répertorier les associations d'identité du pod EKS.	List	cluster*		
ListTagsForResource		Lecture	addon		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée.		capability		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
ListUpdates	Accorde l'autorisation de répertorier les mises à jour pour un Amazon EKS cluster/ nodegroup/add -on donné (dans la région spécifiée ou par défaut)	List	cluster*		
			addon		
			capability		
			nodegroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
MutateViaKubernetesApi [autorisation uniquement]	Accorde l'autorisation de modifier des objets Kubernetes via la console AWS	Écrire	cluster*		eks:AccessKubernetesApi
RegisterCluster	Accorde l'autorisation d'enregistrer un cluster externe	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
StartInsightsRefresh	Autorise le lancement d'une opération d'actualisation à la demande pour obtenir des informations sur le cluster, afin d'obtenir les dernières analyses en dehors du calendrier d'actualisation standard	Écrire	cluster*		
TagResource	Accorde l'autorisation d'identificationr la ressource spécifiée.	Balisage	access-entry		
			addon		
			capability		
			cluster		
			dashboard		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage de la ressource spécifiée.	Identification	access-entry		
			addon		
			capability		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:TagKeys	
UpdateAccessEntry	Accorde l'autorisation de mettre à jour une entrée d'accès Amazon EKS	Écrire	access-entry*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAddon	Accorde l'autorisation de mettre à jour les configurations des modules complémentaires Amazon EKS, comme la version VPC-CNI	Écrire	addon*		
			podidentityassociation		
UpdateCapability	Accorde l'autorisation de mettre à jour une fonctionnalité pour un cluster Amazon EKS	Écrire	capability*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateClusterConfig	Accorde l'autorisation de mettre à jour les configurations des clusters Amazon EKS (par exemple : accès au point de terminaison du serveur d'API)	Écriture	cluster*		
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled eks:loggingType/${type}	
UpdateClusterVersion	Accorde l'autorisation de mettre à jour la version Kubernetes d'un cluster Amazon EKS	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEksAnywhereSubscription	Accorde l'autorisation de mettre à jour un abonnement EKS Anywhere	Écrire	eks-anywhere-subscription*		
UpdateNodegroupConfig	Accorde l'autorisation de mettre à jour les configurations des groupes de nœuds Amazon EKS (par exemple : min/max/desired capacité ou étiquettes)	Écrire	nodegroup*		
UpdateNodegroupVersion	Accorde l'autorisation de mettre à jour la version Kubernetes d'un groupe de nœuds Amazon EKS	Écrire	nodegroup*		
UpdatePodIdentityAssociation	Octroie l'autorisation de mettre à jour une association d'identité du pod EKS.	Écrire	podidentityassociation*		

Types de ressources définis par Amazon Elastic Kubernetes Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
nodegroup	arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}	aws:ResourceTag/${TagKey}
addon	arn:${Partition}:eks:${Region}:${Account}:addon/${ClusterName}/${AddonName}/${UUID}	aws:ResourceTag/${TagKey}
fargateprofile	arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}	aws:ResourceTag/${TagKey}
identityproviderconfig	arn:${Partition}:eks:${Region}:${Account}:identityproviderconfig/${ClusterName}/${IdentityProviderType}/${IdentityProviderConfigName}/${UUID}	aws:ResourceTag/${TagKey}
eks-anywhere-subscription	arn:${Partition}:eks:${Region}:${Account}:eks-anywhere-subscription/${UUID}	aws:ResourceTag/${TagKey}
podidentityassociation	arn:${Partition}:eks:${Region}:${Account}:podidentityassociation/${ClusterName}/${UUID}	aws:ResourceTag/${TagKey}
access-entry	arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}	aws:ResourceTag/${TagKey} eks:accessEntryType eks:clusterName

Types de ressources	ARN	Clés de condition
		eks:kubernetesGroups eks:principalArn eks:username
access-policy	arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}	
dashboard	arn:${Partition}:eks:${Region}:${Account}:dashboard/${DashboardName}	aws:ResourceTag/${TagKey}
capability	arn:${Partition}:eks:${Region}:${Account}:capability/${ClusterName}/${CapabilityType}/${CapabilityName}/${UUID}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service définit les clés de condition suivantes, que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'une clé qui est présente dans la demande envoyée par l'utilisateur au service EKS	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction d'une paire de clé et de valeur de balise	Chaîne
aws:TagKeys	Filtre l'accès en fonction de la liste de tous les noms de clé de balise présents dans la demande envoyée par l'utilisateur au service EKS	ArrayOfString
eks:accessEntryType	Filtre l'accès en fonction du type d'entrée d'accès présent dans les demandes d'entrée d'accès envoyées par l'utilisateur au service EKS	String
eks:accessScope	Filtre l'accès en fonction du paramètre accessScope présent dans la demande de stratégie d'accès dissociée envoyée par l'utilisateur au service EKS	String
eks:authenticationMode	Filtre l'accès selon le mode d'authentification présent dans la demande de cluster de création/mise à jour	String
eks:blockStorageEnabled	Filtre l'accès en fonction du paramètre activé pour le stockage par blocs dans la demande de cluster de création/mise à jour	Booléen
eks:bootstrapClusterCreatorAdminPermissions	Filtre l'accès par le bootstrapClusterCreator AdminPermissions présent dans la demande de création de cluster	Booléen
eks:bootstrapSelfManagedAddons	Filtre l'accès par les bootstrapSelfManaged addons présents dans la demande de création de cluster	Booléen
eks:clientId	Filtre l'accès en fonction du ClientiD présent dans la demande associateIdentityProvider Config envoyée par l'utilisateur au service EKS	String

Clés de condition	Description	Type
eks:clusterName	Filtre l'accès en fonction du paramètre clusterName présent dans les demandes d'entrée d'accès envoyées par l'utilisateur au service EKS	String
eks:computeConfigEnabled	Filtre l'accès par le paramètre compute config activé dans la demande de cluster de création/mise à jour	Booléen
eks:elasticLoadBalancingEnabled	Filtre l'accès en fonction du paramètre activé par Elastic Load Balancing dans la demande de cluster de création/mise à jour	Booléen
eks:issuerUrl	Filtre l'accès en fonction de l'adresse IssuerURL présente dans la demande associateIdentityProvider Config envoyée par l'utilisateur au service EKS.	String
eks:kubernetesGroups	Filtre l'accès en fonction du paramètre kubernetesGroups présent dans les demandes d'entrée d'accès envoyées par l'utilisateur au service EKS	ArrayOfString
eks:loggingType/${type}	Filtre l'accès en fonction de l'activation de la journalisation du cluster et du paramètre de saisie dans la demande de création ou de mise à jour du cluster	Booléen
eks:namespaces	Filtre l'accès en fonction du paramètre namespaces présent dans la demande de stratégie d'accès dissociée envoyée par l'utilisateur au service EKS	ArrayOfString
eks:policyArn	Filtre l'accès en fonction du paramètre policyArn présent dans les demandes d'entrée d'accès envoyées par l'utilisateur au service EKS	ARN
eks:principalArn	Filtre l'accès en fonction du paramètre principalArn présent dans les demandes d'entrée d'accès envoyées par l'utilisateur au service EKS	ARN
eks:supportType	Filtre l'accès en fonction du SupportType présent dans la demande de cluster de création/mise à jour	String

Clés de condition	Description	Type
eks:username	Filtre l'accès en fonction du nom d'utilisateur Kubernetes présent dans les demandes d'entrée d'accès envoyées par l'utilisateur au service EKS	String

Actions, ressources et clés de condition pour AWS Elastic Load Balancing

AWS Elastic Load Balancing (préfixe de service :`elasticloadbalancing`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elastic Load Balancing
- Types de ressources définis par AWS Elastic Load Balancing
- Clés de condition pour AWS Elastic Load Balancing

Actions définies par AWS Elastic Load Balancing

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTags	Accorde l'autorisation d'ajouter des identification spécifiées à l'équilibreur de charge Chaque équilibreur de charge peut disposer de 10 balises au maximum.	Identification	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Accorde l'autorisation pour associer un ou plusieurs groupes de sécurité à votre équilibreur de charge dans un Cloud privé virtuel (VPC).	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
AttachLoadBalancerToSubnets	Accorde l'autorisation d'ajouter une ou plusieurs sous-réseaux à l'ensemble des sous-réseaux configurés pour l'équilibreur de charge spécifié.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConfigureHealthCheck	Accorde des autorisations afin d'indiquer les paramètres de surveillance de l'état à utiliser lors de l'évaluation de l'état de santé de vos instances principales.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateAppCookieStickinessPolicy	Accorde l'autorisation de Générer une politique de permanence avec une durée de vie des sessions permanentes conforme à celle d'un cookie généré par l'application.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLBCookieStickinessPolicy	Accorde l'autorisation de Générer une politique de permanence avec la durée de vie des sessions permanentes contrôlée par la durée de vie du navigateur (utilisateur-agent) ou une période d'expiration précise.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLoadBalancer	Accorde l'autorisation de créer un équilibreur de charge	Écrire	loadbalancer		elasticloadbalancing:AddTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme elasticloadbalanci	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ng:ListenerProtocol	
CreateLoadBalancerListeners	Accorde l'autorisation de créer un ou plusieurs écouteurs pour l'équilibreur de charge spécifié.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	Accorde l'autorisation de créer une politique avec les attributs précis pour l'équilibreur de charge spécifié.	Écrire	loadbalancer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	Accorde l'autorisation de supprimer l'équilibreur de charge spécifié.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLoadBalancerListeners	Accorde l'autorisation de supprimer les écouteurs spécifiés de l'équilibreur de charge indiqué.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	Accorde l'autorisation de supprimer les écouteurs spécifiés de l'équilibreur de charge indiqué. Cette politique ne doit être activée pour aucun écouteur.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterInstancesFromLoadBalancer	Accorde l'autorisation d'annuler l'enregistrement des instances spécifiées de l'équilibreur de charge indiqué.	Écrire	loadbalancer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	Accorde l'autorisation pour décrire l'état des instances spécifiées par rapport à l'équilibreur de charge indiqué.	Lecture			
DescribeLoadBalancerAttributes	Accorde l'autorisation pour décrire les attributs de l'équilibreur de charge spécifié.	Lecture			
DescribeLoadBalancerPolicies	Accorde l'autorisation pour décrire les politiques spécifiées	Lecture			
DescribeLoadBalancerPolicyTypes	Accorde l'autorisation pour décrire les types de politiques d'équilibreur de charge spécifiés.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeLoadBalancers	Accorde l'autorisation pour décrire les l'équilibreurs de charge spécifiés. Si aucun équilibreur de charge n'est spécifié, l'appel décrit tous vos équilibreurs de charge.	List			
DescribeTags	Accorde l'autorisation pour décrire les balises associées aux équilibreurs de charge spécifiés.	Lecture			
DetachLoadBalancerFromSubnets	Accorde l'autorisation pour supprimer les sous-réseaux spécifiés de l'ensemble des sous-réseaux configurés pour l'équilibreur de charge.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableAvailabilityZonesForLoadBalancer	Accorde l'autorisation pour supprimer les zones de disponibilité spécifiées de l'ensemble des zones de disponibilité de l'équilibreur de charge indiqué.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
EnableAvailabilityZonesForLoadBalancer	Accorde l'autorisation d'ajouter les zones de disponibilité spécifiées à l'ensemble des zones de disponibilité de l'équilibreur de charge indiqué.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Accorde l'autorisation de modifier les attributs de l'équilibreur de charge spécifié.	Écrire	loadbalancer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	Accorde l'autorisation d'ajouter des instances spécifiées à l'équilibreur de charge indiqué	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Accorde l'autorisation de supprimer une ou plusieurs identifications de l'équilibreur de charge	Identification	loadbalancer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerListenerSSLCertificate	Accorde l'autorisation pour définir le certificat qui résilie les connexions SSL de l'écouteur spécifié.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetLoadBalancerPoliciesForBackendServer	Accorde l'autorisation de remplacer l'ensemble de politiques associés au port spécifié sur lequel le serveur back-end écoute par un nouvel ensemble de stratégies.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesOfListener	Accorde l'autorisation de remplacer l'ensemble de stratégies actuel pour le port de d'équilibreur de charge indiqué par l'ensemble de stratégies spécifiées.	Écrire	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

Types de ressources définis par AWS Elastic Load Balancing

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Clés de condition pour AWS Elastic Load Balancing

AWS Elastic Load Balancing définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
elasticloadbalancing:CreateAction	Filtre l'accès en fonction du nom d'une action d'API de création de ressources.	String
elasticloadbalancing:ListenerProtocol	Filtre l'accès par les protocoles d’écouteur autorisés dans la demande	ArrayOfString
elasticloadbalancing:ResourceTag/	Filtre l'accès en fonction de la chaîne de préface pour une paire de clés et de valeurs d'identification attachées à une ressource	String
elasticloadbalancing:ResourceTag/${TagKey}	Filtre l'accès en fonction de la chaîne de préface pour une paire de clés et de valeurs d'identification attachées à une ressource	String
elasticloadbalancing:Scheme	Filtre l'accès par le schéma d'équilibrage de charge autorisé dans la demande	String
elasticloadbalancing:SecurityGroup	Filtre l'accès en fonction du groupe de sécurité IDs autorisé dans la demande	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filtre l'accès par les stratégies de sécurité SSL autorisées dans la demande	ArrayOfString
elasticloadbalancing:Subnet	Filtre l'accès par le sous-réseau IDs autorisé dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 (préfixe de service :`elasticloadbalancing`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elastic Load Balancing V2
- Types de ressources définis par AWS Elastic Load Balancing V2
- Clés de condition pour AWS Elastic Load Balancing V2

Actions définies par AWS Elastic Load Balancing V2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddListenerCertificates	Accorde l'autorisation d'ajouter les certificats spécifiés à l'écouteur sécurisé indiqué.	Écrire	listener/app*		
			listener/net*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AddTags	Accorde l'autorisation d'ajouter des identification spécifiées à l'équilibreur de charge Chaque équilibreur de charge peut disposer de 10 balises au maximum.	Identification	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			loadbalancer/net/		
			targetgroup		
			truststore		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTrustStoreRevocations	Octroie l'autorisation d'ajouter des révocations à un magasin d'approbations.	Écrire	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux vendus pour les équilibreurs de charge	Gestion des autorisations			
CreateListener	Accorde l'autorisation de créer un écouteur pour l'Application Load Balancer spécifié.	Écrire	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLoadBalancer	Accorde l'autorisation de créer un équilibreur de charge	Écrire	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRule	Accorde l'autorisation de créer une règle à utiliser pour un écouteur spécifié.	Écrire	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	Accorde l'autorisation de créer un groupe cible	Écrire	targetgroup*		elasticloadbalancing:AddTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	Octroie l'autorisation de créer un magasin d'approbations.	Écrire	truststore		elasticloadbalancing:AddTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateWebACLAssociation [autorisation uniquement]	Accorde l'autorisation d'associer WAF WebACL à l'équilibreur de charge spécifié	Écrire	loadbalancer/app/*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteListener	Accorde l'autorisation de supprimer l'écouteur spécifié	Écrire	listener/app*		
			listener/gwy*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancer	Accorde l'autorisation de supprimer l'équilibreur de charge spécifié.	Écrire	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteRule	Accorde l'autorisation de supprimer la règle spécifiée	Écrire	listener-rule/app*		
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteSharedTrustStoreAssociation	Accorde l'autorisation de supprimer l'association de magasins de confiance partagés spécifiée	Écrire	truststore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTargetGroup	Accorde l'autorisation de supprimer le groupe d'objets spécifié	Écrire	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	Octroie l'autorisation de supprimer le magasin d'approbations spécifié.	Écrire	truststore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteWebACLAssociation [autorisation uniquement]	Accorde l'autorisation de dissocier WAF WebACL de l'équilibreur de charge spécifié	Écrire	loadbalancer/app/*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterTargets	Annule l'enregistrement des cibles spécifiées du groupe cible indiqué.	Écrire	targetgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	Accorde l'autorisation de décrire les limites de ressources d'Elastic Load Balancing pour le Compte AWS	Lecture			
DescribeCapacityReservation	Accorde l'autorisation de décrire la réservation de capacité pour un équilibreur de charge	Lecture			
DescribeListenerAttributes	Accorde l'autorisation de décrire les attributs de l'écouteur spécifié	Lecture			
DescribeListenerCertificates	Accorde l'autorisation de décrire les certificats de l'écouteur sécurisé spécifié.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeListeners	Décrit les écouteurs spécifiés ou les écouteurs de l'Application Load Balancer indiqué.	Lecture			
DescribeLoadBalancerAttributes	Accorde l'autorisation pour décrire les attributs de l'équilibreur de charge spécifié.	Lecture			
DescribeLoadBalancers	Accorde l'autorisation pour décrire les l'équilibreurs de charge spécifiés. Si aucun équilibreur de charge n'est spécifié, l'appel décrit tous vos équilibreurs de charge.	List			
DescribeRules	Accorde l'autorisation de décrire les règles spécifiées ou les règles de l'écouteur indiqué.	Lecture			
DescribeSSLPolicies	Décrit les stratégies spécifiées ou toutes les stratégies utilisées pour la négociation SSL.	Lecture			
DescribeTags	Accorde l'autorisation de décrire les balises associées aux ressources Direct Connect spécifiées.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTargetGroupAttributes	Accorde l'autorisation de décrire les groupes cibles pour le groupe Auto Scaling spécifié.	Lecture			
DescribeTargetGroups	Décrit les groupes cibles spécifiés ou tous vos groupes cibles.	Lecture			
DescribeTargetHealth	Décrit l'état des cibles spécifiées ou de toutes vos cibles.	Lecture			
DescribeTrustStoreAssociations	Octroie l'autorisation de décrire les associations avec un magasin d'approbations.	Lecture			
DescribeTrustStoreRevocations	Octroie l'autorisation de décrire les révocations de magasins d'approbations spécifiés ou toutes vos révocations liées à un magasin d'approbations.	Lecture			
DescribeTrustStores	Octroie l'autorisation de décrire les magasins d'approbations spécifiés ou tous vos magasins d'approbations.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWebACLAssociation [autorisation uniquement]	Permet de décrire tous les équilibreurs de charge associés à un WAF WebACL dans votre compte	List			
GetLoadBalancerWebACL [autorisation uniquement]	Accorde l'autorisation de récupérer le WAF WebACL associé à l'équilibreur de charge spécifié	Lecture	loadbalancer/app/*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetResourcePolicy	Accorde l'autorisation de récupérer la politique de ressource associée à la ressource	Lecture	truststore		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTrustStoreCaCertificatesBundle	Octroie l'autorisation de récupérer une offre groupée de certificats CA de magasin d'approbations.	Lecture	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreRevocationContent	Octroie l'autorisation de récupérer le contenu de révocation d'un magasin d'approbations.	Lecture	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyCapacityReservation	Accorde l'autorisation de modifier la réservation de capacité pour un équilibreur de charge	Écrire	loadbalancer/app/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyIpPools	Accorde l'autorisation de modifier les pools d'adresses IP pour un équilibreur de charge	Écrire	loadbalancer/app/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyListener	Accorde l'autorisation de modifier les propriétés spécifiées de l'écouteur indiqué.	Écrire	listener/app*		
			listener/gwy*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyListenerAttributes	Accorde l'autorisation de modifier les attributs de l'écouteur spécifié	Écrire	listener/app*		
			listener/gwy*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Accorde l'autorisation de modifier les attributs de l'équilibreur de charge spécifié.	Écrire	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyRule	Accorde l'autorisation de désactiver la règle spécifiée	Écrire	listener-rule/app*		
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyTargetGroup	Modifie les vérifications de l'état utilisées lors de l'évaluation de l'état de santé des cibles dans le groupe cible spécifié.	Écrire	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroupAttributes	Accorde l'autorisation de modifier les attributs spécifiés du groupe cible indiqué.	Écrire	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	Octroie l'autorisation de modifier le magasin d'approbations spécifié.	Écrire	truststore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	Accorde l'autorisation d'enregistrer les cibles spécifiées auprès du groupe cible indiqué.	Écrire	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	Accorde l'autorisation de supprimer la politique spécifiée du certificat spécifié	Écrire	listener/app*		
			listener/net*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Accorde l'autorisation de supprimer une ou plusieurs identifications de l'équilibreur de charge	Identification	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			loadbalancer/net/		
			targetgroup		
			truststore		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTrustStoreRevocations	Octroie l'autorisation de supprimer les révocations d'un magasin d'approbations.	Écrire	truststore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetIpAddressType	Accorde l'autorisation de définir le type d'adresses IP utilisées par les sous-réseaux de l'équilibreur de charge indiqué.	Écrire	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetRulePriorities	Accorde l'autorisation de définir les priorités des règles spécifiées	Écrire	listener-rule/app*		
			listener-rule/net*		
SetSecurityGroups	Accorde l'autorisation d'associer les groupes de sécurité spécifiés à l'équilibreur de charge indiqué.	Écrire	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	Active la zone de disponibilité des sous-réseaux spécifiés pour l'équilibreur de charge indiqué.	Écrire	loadbalancer/app/		
			loadbalancer/gwy/		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [autorisation uniquement]	Donne l'autorisation de donner WebAcl l'autorisation à WAF	Écrire			

Types de ressources définis par AWS Elastic Load Balancing V2

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
listener/gwy	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/gwy/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
loadbalancer/gwy/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/gwy/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/net/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
targetgroup	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:targetgroup/${TargetGroupName}/${TargetGroupId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
truststore	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:truststore/${TrustStoreName}/${TrustStoreId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Clés de condition pour AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
elasticloadbalancing:CreateAction	Filtre l'accès en fonction du nom d'une action d'API de création de ressources.	String
elasticloadbalancing:ListenerProtocol	Filtre l'accès par le protocole d'écouteur autorisé dans la requête	String
elasticloadbalancing:ResourceTag/${TagKey}	Filtre l'accès en fonction de la chaîne de préface pour une paire de clés et de valeurs d'identification attachées à une ressource	String
elasticloadbalancing:Scheme	Filtre l'accès par le schéma d'équilibrage de charge autorisé dans la demande	String

Clés de condition	Description	Type
elasticloadbalancing:SecurityGroup	Filtre l'accès en fonction du groupe de sécurité IDs autorisé dans la demande	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filtre l'accès par les stratégies de sécurité SSL autorisées dans la demande	ArrayOfString
elasticloadbalancing:Subnet	Filtre l'accès par le sous-réseau IDs autorisé dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Elastic MapReduce

Amazon Elastic MapReduce (préfixe de service :`elasticmapreduce`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic MapReduce
- Types de ressources définis par Amazon Elastic MapReduce
- Clés de condition pour Amazon Elastic MapReduce

Actions définies par Amazon Elastic MapReduce

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> L' DescribeJobFlows API est obsolète et sera finalement supprimée. Nous vous recommandons d'utiliser ListClusters, DescribeCluster ListSteps, ListInstanceGroups et à la ListBootstrapActions place

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AccessAllEventLogs	Autorise l'affichage de tous les journaux d'événements sur un serveur d'historique permanent des applications	Écrire	cluster*		
AddInstanceFleet	Accorde l'autorisation d'ajouter un parc d'instances à un cluster en cours d'exécution	Écrire	cluster*		
AddInstanceGroups	Accorde l'autorisation d'ajouter des groupes d'instances à un cluster en cours d'exécution	Écrire	cluster*		
AddJobFlowSteps	Accorde l'autorisation d'ajouter de nouvelles étapes à un cluster en cours d'exécution	Écrire	cluster*		
				elasticmapreduce:ExecutionRoleArn	
AddTags	Accorde l'autorisation d'ajouter des balises à une ressource Amazon EMR	Identification	cluster		
			editor		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			notebook-execution		
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
AttachEditor [autorisation uniquement]	Accorde l'autorisation d'attacher un EMR Notebook à un moteur de calcul	Écrire	editor*		
CancelSteps	Accorde l'autorisation d'annuler une étape ou des étapes en attente dans un cluster en cours d'exécution	Écrire	cluster*		
CreateEditor [autorisation uniquement]	Accorde l'autorisation de créer un EMR Notebook	Écrire	cluster		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreatePersistentAppUI	Accorde l'autorisation de créer un serveur d'historique d'applications persistant	Écrire	cluster*		
CreateRepository [autorisation uniquement]	Accorde l'autorisation de créer un référentiel EMR Notebook	Écrire			
CreateSecurityConfiguration	Accorde l'autorisation de créer une configuration de sécurité.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateStudio	Accorde l'autorisation de créer un EMR Studio	Écrire		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	Autorise le lancement d'un EMR Studio à l'aide du mode d'authentification IAM	Écrire	studio*		
CreateStudioSessionMapping	Accorde l'autorisation de créer un mappage de session EMR Studio	Écrire	studio*		
DeleteEditor [autorisation uniquement]	Accorde l'autorisation de supprimer un EMR Notebook	Écrire	editor*		
DeleteRepository [autorisation uniquement]	Accorde l'autorisation de supprimer un référentiel EMR Notebook	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSecurityConfiguration	Accorde l'autorisation de supprimer une configuration de sécurité.	Écrire			
DeleteStudio	Accorde l'autorisation de supprimer un EMR Studio	Écrire	studio*		
DeleteStudioSessionMapping	Accorde l'autorisation de supprimer un mappage de session EMR Studio	Écrire	studio*		
DeleteWorkspaceAccess [autorisation uniquement]	Accorde l'autorisation d'empêcher une identité d'ouvrir un espace de travail collaboratif	Gestion des autorisations	editor*		
DescribeCluster	Accorde l'autorisation d'obtenir les détails relatifs à un cluster, y compris le statut, la configuration matérielle et logicielle, les paramètres VPC, etc.	Lecture	cluster*		
DescribeEditor [autorisation uniquement]	Accorde l'autorisation d'afficher des informations sur un notebook, y compris le statut, l'utilisateur, le rôle, les balises, l'emplacement, etc.	Lecture	editor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeJobFlows	Accorde l'autorisation de décrire les détails des clusters (flux de travail). Cette API est obsolète et finira par être supprimée. Nous vous recommandons d'utiliser ListClusters, DescribeCluster ListSteps, ListInstanceGroups et à la ListBootstrapActions place	Lecture	cluster*		
DescribeNotebookExecution	Accorde l'autorisation d'afficher des informations relatives à l'exécution d'un notebook	Lecture	notebook-execution*		
DescribePersistentAppUI	Accorde l'autorisation de décrire un serveur d'historique d'applications persistant	Lecture	cluster*		
DescribeReleaseLabel	Accorde l'autorisation d'afficher les informations relatives à une publication EMR, telles que les applications prises en charge	Lecture			
DescribeRepository [autorisation uniquement]	Accorde l'autorisation de décrire un référentiel EMR Notebook	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSecurityConfiguration	Accorde l'autorisation d'obtenir les détails d'une configuration de sécurité	Lecture			
DescribeStep	Accorde l'autorisation d'obtenir les détails relatifs à une étape de cluster	Lecture	cluster*		
DescribeStudio	Accorde l'autorisation d'afficher des informations relatives à un EMR Studio	Lecture	studio*		
DetachEditor [autorisation uniquement]	Accorde l'autorisation de détacher un notebook EMR d'un moteur de calcul	Écrire	editor*		
GetAutoTerminationPolicy	Accorde l'autorisation de récupérer la politique d'arrêt automatique associée à un cluster	Lecture	cluster*		
GetBlockPublicAccessConfiguration	Accorde l'autorisation de récupérer la configuration d'accès public du bloc EMR pour le Compte AWS dans la région	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetClusterSessionCredentials	Accorde l'autorisation de récupérer les informations d'identification HTTP de base associées à un rôle IAM d'exécution donné pour un cluster EMR activé par un contrôle d'accès détaillé	Écrire	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetManagedScalingPolicy	Accorde l'autorisation de récupérer la politique de mise à l'échelle gérée associée à un cluster	Lecture	cluster*		
GetOnClusterAppUIPresignedURL	Autorise à obtenir une URL présignée pour un serveur d'historique des applications exécuté sur le cluster	Écrire	cluster*		
GetPersistentAppUIPresignedURL	Accorde l'autorisation d'obtenir une URL présignée pour un serveur d'historique d'applications persistant	Écrire	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetStudioSessionMapping	Accorde l'autorisation d'afficher des informations sur le mappage d'une session d'EMR Studio	Lecture	studio*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
LinkRepository [autorisation uniquement]	Accorde l'autorisation d'établir la liaison entre un référentiel EMR Notebook et EMR Notebooks	Écrire			
ListBootstrapActions	Accorde l'autorisation d'obtenir des détails sur les actions d'amorçage associées à un cluster	Lecture	cluster*		
ListClusters	Accorde l'autorisation d'obtenir l'état des clusters accessibles	List			
ListEditors [autorisation uniquement]	Accorde l'autorisation de répertorier des informations récapitulatives sur les EMR Notebooks accessibles	List			
ListInstanceFleets	Accorde l'autorisation d'obtenir les détails des parcs d'instances dans un cluster	Lecture	cluster*		
ListInstanceGroups	Accorde l'autorisation d'obtenir des détails sur les groupes d'instances d'un cluster	Lecture	cluster*		
ListInstances	Accorde l'autorisation d'obtenir des détails sur les instances Amazon EC2 dans un cluster	Lecture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNotebookExecutions	Accorde l'autorisation de répertorier des informations récapitulatives pour les exécutions notebook	List			
ListReleaseLabels	Accorde l'autorisation de répertorier et de filtrer les versions EMR disponibles dans la région actuelle	List			
ListRepositories [autorisation uniquement]	Accorde l'autorisation de répertorier des référentiels EMR Notebook existants	List			
ListSecurityConfigurations	Accorde l'autorisation de répertorier les configurations de sécurité disponibles dans ce compte par leur nom, ainsi que leurs date et heure de création	List			
ListSteps	Accorde l'autorisation de répertorier les étapes associées à un cluster	Lecture	cluster*		
ListStudioSessionMappings	Accorde l'autorisation de répertorier des informations récapitulatives sur les mappages de session EMR Studio	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStudios	Accorde l'autorisation de répertorier des informations récapitulatives sur les EMR Studios	List			
ListSupportedInstanceTypes	Accorde l'autorisation de répertorier les types d'instances Amazon EC2 pris en charge par une version Amazon EMR	List			
ListWorkspaceAccessIdentities [autorisation uniquement]	Accorde l'autorisation de répertorier les identités qui ont accès à un espace de travail.	List	editor*		
ModifyCluster	Accorde l'autorisation de modifier les paramètres du cluster, tels que le nombre d'étapes pouvant être exécutées simultanément pour un cluster	Écrire	cluster*		
ModifyInstanceFleet	Accorde l'autorisation de modifier les capacités cibles des instances à la demande et Spot d'un parc d'instances	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyInstanceGroups	Accorde l'autorisation de modifier le nombre et la configuration des instances EC2 pour un groupe d'instances	Écrire	cluster		
OpenEditorInConsole [autorisation uniquement]	Accorde l'autorisation de lancer l'éditeur de blocs-notes Jupyter pour un EMR Notebook à partir de la console	Écrire	editor* cluster		
PutAutoScalingPolicy	Accorde l'autorisation de créer ou de mettre à jour une politique de scalabilité automatique pour un groupe d'instances de base ou un groupe d'instances de tâches	Écrire	cluster*		
PutAutoTerminationPolicy	Accorde l'autorisation de créer ou de mettre à jour la politique d'arrêt automatique associée à un cluster	Écrire	cluster*		
PutBlockPublicAccessConfiguration	Accorde l'autorisation de créer ou de mettre à jour la configuration d'accès public du bloc EMR pour la Compte AWS région	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutManagedScalingPolicy	Accorde l'autorisation de créer ou de mettre à jour la politique de mise à l'échelle gérée associée à un cluster	Écrire	cluster*		
PutWorkspaceAccess [autorisation uniquement]	Accorde l'autorisation d'autoriser une identité à ouvrir un espace de travail collaboratif.	Gestion des autorisations	editor*		
RemoveAutoScalingPolicy	Accorde l'autorisation de supprimer une politique de scalabilité automatique à partir d'un groupe d'instances	Écrire	cluster*		
RemoveAutoTerminationPolicy	Accorde l'autorisation de supprimer la politique d'arrêt automatique associée à un cluster	Écrire	cluster*		
RemoveManagedScalingPolicy	Accorde l'autorisation de supprimer la politique de mise à l'échelle gérée associée à un cluster	Écrire	cluster*		
RemoveTags	Accorde l'autorisation de supprimer des balises d'une ressource Amazon EMR	Identification	cluster		
			editor		
			notebook-execution		
			studio		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
RunJobFlow	Accorde l'autorisation de créer et lancer un cluster (flux de travail)	Écrire		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	Accorde l'autorisation d'ajouter et de supprimer la terminaison automatique après l'exécution d'une étape pour un cluster	Écrire	cluster*		
SetTerminationProtection	Accorde l'autorisation d'ajouter et de supprimer la protection contre l'arrêt pour un cluster	Écrire	cluster*		
SetUnhealthyNodeReplacement	Accorde l'autorisation d'activer ou de désactiver le remplacement de nœuds défectueux pour un cluster	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetVisibleToAllUsers	Accorde l'autorisation de définir si tous les utilisateurs d' AWS Identity and Access Management (IAM) du Compte AWS peuvent voir un cluster. Cette API est obsolète et votre cluster peut être visible par tous les utilisateurs de votre compte. Pour restreindre l'accès au cluster à l'aide d'une politique IAM, consultez AWS Identity and Access Management for Amazon EMR https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr (plan-access-iam- .html)	Écrire	cluster*		
StartEditor [autorisation uniquement]	Accorde l'autorisation de démarrer un EMR Notebook	Écrire	editor*		
			cluster		
StartNotebookExecution	Accorde l'autorisation de démarrer l'exécution d'un EMR Notebook	Écrire	cluster*		
			editor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor [autorisation uniquement]	Accorde l'autorisation d'arrêter un EMR Notebook	Écrire	editor*		
StopNotebookExecution	Accorde l'autorisation d'arrêter l'exécution du notebook	Écrire	notebook-execution*		
TerminateJobFlows	Accorde l'autorisation de résilier un cluster (flux de travail)	Écrire	cluster*		
UnlinkRepository [autorisation uniquement]	Accorde l'autorisation d'annuler le lien entre un référentiel EMR Notebook et EMR Notebooks	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEditor [autorisation uniquement]	Accorde l'autorisation de mettre à jour un EMR Notebook.	Écrire	editor*		
UpdateRepository [autorisation uniquement]	Accorde l'autorisation de mettre à jour un référentiel EMR Notebook	Écrire			
UpdateStudio	Accorde l'autorisation de mettre à jour des informations relatives à un EMR Studio	Écrire	studio*		
UpdateStudioSessionMapping	Accorde l'autorisation de mettre à jour du mappage de session EMR Studio	Écrire	studio*		
ViewEventsFromAllClustersInConsole [autorisation uniquement]	Accorde l'autorisation d'utiliser la console EMR pour afficher des événements de tous les clusters	List			

Types de ressources définis par Amazon Elastic MapReduce

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:cluster/${ClusterId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
editor	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:editor/${EditorId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
notebook-execution	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:notebook-execution/${NotebookExecutionId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
studio	`arn:${Partition}:elasticmapreduce:${Region}:${Account}:studio/${StudioId}`	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}

Clés de condition pour Amazon Elastic MapReduce

Amazon Elastic MapReduce définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès selon que la paire balise et valeur est fournie ou non avec l'action	String
aws:ResourceTag/${TagKey}	Filtre l'accès aux actions en fonction de la paire balise-valeur associée à une ressource Amazon EMR	String
aws:TagKeys	Filtre l'accès selon que les clés de balise sont fournies ou non avec l'action, quelle que soit la valeur de la balise	ArrayOfString
elasticmapreduce:ExecutionRoleArn	Filtre l'accès selon que l'ARN du rôle d'exécution est fourni ou non avec l'action	ARN
elasticmapreduce:RequestTag/${TagKey}	Filtre l'accès selon que la paire balise et valeur est fournie ou non avec l'action	String
elasticmapreduce:ResourceTag/${TagKey}	Filtre l'accès aux actions en fonction de la paire balise-valeur associée à une ressource Amazon EMR	String

Actions, ressources et clés de condition pour Amazon Elastic Transcoder

Amazon Elastic Transcoder (préfixe de service : `elastictranscoder`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic Transcoder
- Types de ressources définis par Amazon Elastic Transcoder
- Clés de condition pour Amazon Elastic Transcoder

Actions définies par Amazon Elastic Transcoder

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelJob	Annule une tâche qu'Elastic Transcoder n'a pas commencé à traiter.	Écrire	job*		
CreateJob	Créez une tâche	Écrire	pipeline*		
			preset*		
CreatePipeline	Crée un pipeline.	Écrire			
CreatePreset	Crée un préréglage	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePipeline	Supprime un pipeline.	Écriture	pipeline*		
DeletePreset	Supprime un préréglage.	Écriture	preset*		
ListJobsByPipeline	Récupère la liste des tâches que vous avez affectées à un pipeline.	List	pipeline*		
ListJobsByStatus	Obtenir des informations sur toutes les tâches associées au poste actuel Compte AWS qui ont un statut spécifique	List			
ListPipelines	Obtenez une liste des pipelines associés au courant Compte AWS	List			
ListPresets	Obtenez une liste de tous les préréglages associés au courant Compte AWS	List			
ReadJob	Récupère des informations détaillées sur une tâche.	Lecture	job*		
ReadPipeline	Récupère des informations détaillées sur un pipeline.	Lecture	pipeline*		
ReadPreset	Récupère des informations détaillées sur un préréglage	Lecture	preset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestRole	Teste les paramètres d'un pipeline afin de s'assurer qu'Elastic Transcoder peut créer et traiter des tâches.	Écriture			
UpdatePipeline	Met à jour les paramètres d'un pipeline.	Écriture	pipeline*		
UpdatePipelineNotifications	Met à jour uniquement les notifications Amazon Simple Notification Service (Amazon SNS) pour un pipeline.	Écrire	pipeline*		
UpdatePipelineStatus	Suspend ou réactive un pipeline, de sorte que celui-ci arrête ou redémarre le traitement des tâches, et met à jour le statut du pipeline	Écrire	pipeline*		

Types de ressources définis par Amazon Elastic Transcoder

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
job	`arn:${Partition}:elastictranscoder:${Region}:${Account}:job/${JobId}`	
pipeline	`arn:${Partition}:elastictranscoder:${Region}:${Account}:pipeline/${PipelineId}`	
preset	`arn:${Partition}:elastictranscoder:${Region}:${Account}:preset/${PresetId}`	

Clés de condition pour Amazon Elastic Transcoder

Elastic Transcoder ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Elastic VMware Service

Amazon Elastic VMware Service (préfixe de service :`evs`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Elastic VMware Service

- Types de ressources définis par Amazon Elastic VMware Service
- Clés de condition pour Amazon Elastic VMware Service

Actions définies par Amazon Elastic VMware Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateEipToVlan	Accorde l'autorisation d'associer une adresse IP élastique (EIP) à un VLAN public dans un environnement Amazon EVS	Écrire	environment*		ec2:AssociateAddress ec2:DescribeAddresses
CreateEnvironment	Accorde l'autorisation de créer un environnement Amazon EVS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateSubnet ec2:CreateTags ec2:DeleteNetworkInterface

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DeleteSubnet ec2:DeleteVolume ec2:DescribeAddresses ec2:DescribeDhcpOptions ec2:DescribeHosts ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeKeyPairs ec2:DescribeNetworkInterfaces

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribePlacementGroups ec2:DescribeRouteServerEndpoints ec2:DescribeRouteServerPeers ec2:DescribeRouteServers ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVolumes ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DetachNetworkInterface ec2:DetachVolume ec2:GetAllowedImagesSettings ec2:GetRouteServerAssociations ec2:ModifyInstanceAttribute ec2:ModifyNetworkInterfaceAttribute ec2:RunInstances ec2:TerminateInstances

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:CreateServiceLinkedRole kms:DescribeKey kms:ListAliases secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:GetRandomPassword secretsmanager:GetSecretValue secretsmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:UpdateSecret servicequotas:GetServiceQuota servicequotas:ListServiceQuotas support:DescribeServices support:DescribeSupportLevel

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEnvironmentHost	Accorde l'autorisation d'ajouter un hôte à un environnement Amazon EVS	Écrire	environment*		ec2:CreateNetworkInterface ec2:CreateTags ec2:DeleteNetworkInterface ec2:DescribeDhcpOptions ec2:DescribeHosts ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeKeyPairs ec2:DescribeNetwor

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					kInterfaces ec2:DescribePlacementGroups ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute ec2:RunInstances evs:CreateEnvironmentHost secretsmanager:CreateSecret

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:DeleteSecret secretsmanager:GetRandomPassword secretsmanager:GetSecretValue secretsmanager:TagResource secretsmanager:UpdateSecret servicequotas:GetServiceQuota servicequotas:ListServiceQuotas

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEnvironment	Accorde l'autorisation de supprimer un environnement Amazon EVS	Écrire	environment*		ec2:DeleteNetworkInterface ec2:DeleteSubnet ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyInstanceAttribute ec2:ModifyNetworkInterfaceAttribute

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:TerminateInstances secretsmanager:DeleteSecret secretsmanager:GetSecretValue

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEnvironmentHost	Accorde l'autorisation de supprimer un hôte d'un environnement Amazon EVS	Écrire	environment*		ec2:DeleteNetworkInterface ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeNetworkInterfaces ec2:ModifyInstanceAttribute ec2:ModifyNetworkInterfaceAttribute ec2:TerminateInstances secretsmanager:DeleteSecret

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:GetSecretValue
DisassociateEipFromVlan	Accorde l'autorisation de dissocier une adresse IP élastique (EIP) d'un VLAN public dans un environnement Amazon EVS	Écrire	environment*		ec2:DisassociateAddress
GetEnvironment	Accorde l'autorisation d'obtenir un environnement Amazon EVS	Lecture	environment*		
GetVersions	Accorde l'autorisation d'obtenir les versions fournies pour le lancement par Amazon EVS	Lecture			
ListEnvironmentHosts	Accorde l'autorisation de récupérer une liste d'hôtes associés à un environnement Amazon EVS	List	environment*		
ListEnvironmentVlans	Accorde l'autorisation de récupérer une liste de l'environnement Amazon EVS VLANs	List	environment*		
ListEnvironments	Accorde l'autorisation de récupérer la liste des environnements Amazon EVS dans un compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises sur l'ARN d'une ressource spécifiée	Lecture	environment		
TagResource	Accorde l'autorisation de baliser l'ARN d'une ressource spécifiée	Identification	environment*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises de l'ARN d'une ressource spécifiée	Identification	environment*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Types de ressources définis par Amazon Elastic VMware Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
environment	`arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentIdentifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Elastic VMware Service

Amazon Elastic VMware Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour Amazon ElastiCache

Amazon ElastiCache (préfixe de service :`elasticache`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon ElastiCache
- Types de ressources définis par Amazon ElastiCache
- Clés de condition pour Amazon ElastiCache

Actions définies par Amazon ElastiCache

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> Lorsque vous créez une ElastiCache politique dans IAM, vous devez utiliser le caractère générique « * » pour le bloc de ressources. Pour plus d'informations sur l'utilisation des actions d' ElastiCache API suivantes dans une politique IAM, consultez ElastiCache Actions et IAM dans le guide de ElastiCache l'utilisateur Amazon.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTagsToResource	Accorde l'autorisation d'ajouter des balises à une ElastiCache ressource	Identification	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
Authorize CacheSecurityGroupIngress	Accorde l'autorisation d'autoriser un groupe de sécurité EC2 sur un groupe ElastiCache de sécurité	Écrire	securitygroup*		ec2:AuthorizeSecurityGroupIngress
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchApplyUpdateAction	Accorde l'autorisation d'appliquer des mises à jour de ElastiCache service à des ensembles de clusters et de groupes de réplication	Écrire	cluster		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
			replicationgroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchStopUpdateAction	Accorde l'autorisation d'arrêter l'exécution des mises à jour de ElastiCache service sur un ensemble de clusters	Écrire	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CompleteMigration	Accorde l'autorisation d'effectuer une migration en ligne des données depuis Redis hébergé sur Amazon EC2 vers ElastiCache	Écrire	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
Connect	Accorde l'autorisation de se connecter en tant qu' ElastiCache utilisateur spécifié à un groupe de ElastiCache réplication ou à un ElastiCache cache sans serveur	Écrire	user*		
			replicationgroup		
			serverlesscache		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CopyServerlessCacheSnapshot	Octroie l'autorisation de faire une copie d'un instantané de cache sans serveur existant.	Écrire	serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshot	Accorde l'autorisation de faire une copie d'un instantané existant.	Écriture	snapshot*		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCacheCluster	Accorde l'autorisation de créer un cluster de cache.	Écriture	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			cluster	aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticache:CacheParameterGroupName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			replicationgroup	elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			securitygroup		
			snapshot		
			subnetgroup		
				aws:ResourceTag/${TagKey}	
CreateCacheParameterGroup	Accorde l'autorisation de créer un groupe de paramètres.	Écriture	parametergroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCacheSecurityGroup	Accorde l'autorisation de créer un groupe de sécurité de cache.	Écriture	securitygroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCacheSubnetGroup	Accorde l'autorisation de créer un groupe de sous-réseaux de cache.	Écriture	subnetgroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGlobalReplicationGroup	Accorde l'autorisation de créer un groupe de réplication global.	Écriture	globalreplicationgroup*		
			replicationgroup*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReplicationGroup	Accorde l'autorisation de créer un groupe de réplication.	Écrire	parametergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject
			cluster		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			globalreplicationgroup	elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:TransitEncryptionEnabled elasticache:Automa	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			replicationgroup	aws:RequestTag/${TagKey} aws:TagKeys elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticache:TransitEncryptionEnabled elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticache:CacheParameterGroupName	
			securitygroup		
			snapshot		
			subnetgroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateServerlessCache	Octroie l'autorisation de créer un cache sans serveur.	Écrire	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineType elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataSt	ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTags ec2:DescribeVpcEndpoints ec2:DescribeVpcs elasticache:AddTagsToResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				orageUnit elasticache:MinimumECPUPerSecond elasticache:MaximumECPUPerSecond	s3:GetObject
			serverlesscachesnapshot	aws:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey}	
			usergroup	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateServerlessCacheSnapshot	Octroie l'autorisation de créer une copie d'un cache sans serveur à un moment précis.	Écrire	serverlesscache*	aws:ResourceTag/${TagKey}	elasticache:AddTagsToResource
			serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Accode l'autorisation de créer une copie d'un cluster Redis entier à un moment précis.	Écrire	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CreateUser	Accorde l'autorisation de créer un utilisateur pour Redis. Les utilisateurs sont pris en charge à partir de la version Redis 6.0.	Écrire	user*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUserGroup	Accorde l'autorisation de créer un groupe d'utilisateurs pour Redis. Les groupes sont pris en charge à partir de la version Redis 6.0.	Écrire	user*		elasticache:AddTagsToResource
			usergroup*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	
DecreaseNodeGroupsInGlobalReplicationGroup	Accorde l'autorisation de réduire le nombre de groupes de nœuds dans les groupes de réplication globaux.	Écriture	globalreplicationgroup*		
				elasticache:NumNodeGroups	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DecreaseReplicaCount	Accorde l'autorisation de réduire le nombre de réplicas dans un groupe de réplication Redis (mode cluster désactivé) ou le nombre de nœuds de réplica dans un ou plusieurs groupes de nœuds (partitions) d'un groupe de réplication Redis (mode cluster activé).	Écriture	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCacheCluster	Accorde l'autorisation de supprimer un cluster précédemment provisionné	Écriture	cluster*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteCacheParameterGroup	Accorde l'autorisation de supprimer le groupe de paramètres de cache spécifié.	Écriture	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCacheSecurityGroup	Accorde l'autorisation de supprimer un groupe de sécurité de cache.	Écriture	securitygroup*		
				aws:ResourceTag/${TagKey}	
DeleteCacheSubnetGroup	Accorde l'autorisation de supprimer un groupe de sous-réseaux de cache.	Écriture	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteGlobalReplicationGroup	Accorde l'autorisation de supprimer un groupe de réplication global existant.	Écriture	globalreplicationgroup*		
DeleteReplicationGroup	Accorde l'autorisation de supprimer un groupe de réplication existant.	Écrire	replicationgroup*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteServerlessCache	Octroie l'autorisation de supprimer un cache sans serveur.	Écrire	serverlesscache*	aws:ResourceTag/${TagKey}	ec2:DescribeTags
			serverlesscachesnapshot		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteServerlessCacheSnapshot	Octroie l'autorisation de supprimer un instantané de cache sans serveur.	Écrire	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	
DeleteSnapshot	Accorde l'autorisation de supprimer un instantané existant.	Écriture	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteUser	Accorde l'autorisation de supprimer un utilisateur existant et donc de le supprimer de tous les groupes d'utilisateurs et groupes de réplication auxquels il a été affecté.	Écriture	user*		
				aws:ResourceTag/${TagKey}	
DeleteUserGroup	Accorde l'autorisation de supprimer un groupe d'utilisateurs existant.	Écriture	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheClusters	Accorde l'autorisation de répertorier des informations sur les clusters de cache provisionnés.	List	cluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCacheEngineVersions	Accorde l'autorisation de répertorier les moteurs de cache disponibles et leurs versions	List			
DescribeCacheParameterGroups	Accorde l'autorisation de répertorier les descriptions de groupes de paramètres de cache.	Liste	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheParameters	Accorde l'autorisation de renvoyer la liste détaillée des paramètres pour un groupe de paramètres de cache particulier.	Liste	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSecurityGroups	Accorde l'autorisation de répertorier les descriptions de groupes de sécurité.	Liste	securitygroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSubnetGroups	Accorde l'autorisation de répertorier les descriptions de groupes de sous-réseaux de cache.	Liste	subnetgroup*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEngineDefaultParameters	Accorde l'autorisation de récupérer les informations sur les paramètres de moteur et système par défaut du moteur de cache spécifié.	Liste			
DescribeEvents	Accorde l'autorisation de répertorier les événements liés aux clusters, aux groupes de sécurité de cache et aux groupes de paramètres de cache.	Liste			
DescribeGlobalReplicationGroups	Accorde l'autorisation de répertorier des informations sur les groupes de réplication globaux.	Liste	globalreplicationgroup*		
DescribeReplicationGroups	Accorde l'autorisation de répertorier des informations sur les groupes de réplication provisionnés.	Liste	replicationgroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodes	Accorde l'autorisation de répertorier des informations sur les nœuds de cache réservés achetés.	Liste	reserved-instance*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReservedCacheNodesOfferings	Accorde l'autorisation de répertorier les offres de nœuds de cache réservés.	List			
DescribeServerlessCacheSnapshots	Octroie l'autorisation de répertorier des informations sur des instantanés de cache sans serveur.	List	serverlessscachesnapshot*	aws:ResourceTag/${TagKey}	
			serverlesscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	Octroie l'autorisation de répertorier des caches sans serveur.	List	serverlesscache*	aws:ResourceTag/${TagKey}	
DescribeServiceUpdates	Accorde l'autorisation de répertorier les détails des mises à jour du service.	Liste			
DescribeSnapshots	Accorde l'autorisation de répertorier des informations sur les instantanés de cluster ou de groupe de réplication.	Liste	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeUpdateActions	Accorde l'autorisation de répertorier les détails des actions de mise à jour pour un ensemble de clusters ou de groupes de réplication.	Liste	cluster		
			replicationgroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DescribeUserGroups	Accorde l'autorisation de répertorier des informations sur les groupes d'utilisateurs Redis.	Liste	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Accorde l'autorisation de répertorier des informations sur les utilisateurs Redis.	Liste	user*		
				aws:ResourceTag/${TagKey}	
DisassociateGlobalReplicationGroup	Accorde l'autorisation de supprimer un groupe de réplication secondaire du groupe de réplication global.	Écrire	globalreplicationgroup*		
ExportServerlessCacheSnapshot	Octroie l'autorisation d'exporter une copie d'un cache sans serveur à un moment précis vers un compartiment s3.	Écrire	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	s3:DeleteObject s3:ListAllMyBuckets s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
FailoverGlobalReplicationGroup	Autorise le basculement de la région principale vers une région secondaire sélectionnée d'un groupe de réplication global.	Écriture	globalreplicationgroup*		
IncreaseNodeGroupsInGlobalReplicationGroup	Accorde l'autorisation d'augmenter le nombre de groupes de nœuds dans un groupe de réplication global.	Écriture	globalreplicationgroup*		
				elasticache:NumNodeGroups	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
IncreaseReplicaCount	Accorde l'autorisation d'augmenter le nombre de réplicas dans un groupe de réplication Redis (mode cluster désactivé) ou le nombre de nœuds de réplica dans un ou plusieurs groupes de nœuds (partitions) d'un groupe de réplication Redis (mode cluster activé).	Écrire	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InterruptClusterAzPower [autorisation uniquement]	Accorde l'autorisation de tester une interruption de courant AZ pour une ElastiCache ressource	Écrire	replicationgroup*		
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeModifications	Accorde l'autorisation de répertorier le type de nœud disponible qui peut être utilisé pour mettre à l'échelle un cluster Redis particulier ou un groupe de réplication.	List	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ElastiCache ressource	Lecture	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyCacheCluster	Accorde l'autorisation de modifier les paramètres d'un cluster.	Écriture	cluster*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			parametergroup		
			securitygroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	Accorde l'autorisation de modifier les paramètres d'un groupe de paramètres de cache.	Écriture	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
ModifyCacheSubnetGroup	Accorde l'autorisation de modifier un groupe de sous-réseaux de cache existant.	Écriture	subnetgroup*		
				aws:ResourceTag/${TagKey}	
ModifyGlobalReplicationGroup	Accorde l'autorisation de modifier les paramètres d'un groupe de réplication global.	Écriture	globalreplicationgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyReplicationGroup	Accorde l'autorisation de modifier les paramètres d'un groupe de réplication.	Écriture	replicationgroup*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticache:TransitEncryptionEnabled elasticache:ClusterModeEnabled	
			parametergroup		
			securitygroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyReplicationGroupShardConfiguration	Accorde l'autorisation d'ajouter des partitions, de supprimer des partitions ou de rééquilibrer les espaces de clés entre les partitions existantes d'un groupe de réplication.	Écrire	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:NumNodeGroups	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyServerlessCache	Octroie l'autorisation de modifier les paramètres d'un cache sans serveur.	Écrire	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MinimumECPUPerSecond	ec2:DescribeSecurityGroups ec2:DescribeTags

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				elasticache:MaximumECPUPerSecond	
			usergroup	aws:ResourceTag/${TagKey}	
ModifyUser	Accorde l'autorisation de modifier la chaîne d' and/or accès au (x) mot (s) de passe utilisateur Redis	Écrire	user*		
				aws:ResourceTag/${TagKey} elasticache:UserAuthenticationMode	
ModifyUserGroup	Accorde l'autorisation de modifier la liste des utilisateurs appartenant au groupe d'utilisateurs.	Écriture	user*		
			usergroup*		
				aws:ResourceTag/${TagKey}	
PurchaseReservedCacheNodesOffering	Accorde l'autorisation d'acheter une offre de nœud de cache réservé.	Écriture	reserved-instance*		elasticache:AddTagsToResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RebalanceSlotsInGlobalReplicationGroup	Accorde l'autorisation d'effectuer une opération de rééquilibrage de l'espace de clés pour redistribuer les intervalles et garantir une distribution uniforme des clés entre les partitions existantes dans un groupe de réplication global.	Écriture	globalreplicationgroup*		
RebootCacheCluster	Accorde l'autorisation de redémarrer une partie ou la totalité des nœuds de cache au sein d'un cluster de cache provisionné ou d'un groupe de réplication (mode cluster désactivé).	Écrire	cluster*		
				aws:ResourceTag/${TagKey}	
RemoveTagsFromResource	Accorde l'autorisation de supprimer des balises d'une ElastiCache ressource	Identification	cluster		
			parameter group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResetCacheParameterGroup	Accorde l'autorisation de modifier des paramètres d'un groupe de paramètres de cache à leurs valeurs par défaut.	Écrire	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
RevokeCacheSecurityGroupIngress	Accorde l'autorisation de supprimer une entrée de groupe de sécurité EC2 d'un ElastiCache groupe de sécurité	Écrire	securitygroup*		
				aws:ResourceTag/${TagKey}	
StartMigration	Autorise le lancement d'une migration de données depuis Redis hébergé sur Amazon EC2 ElastiCache vers Redis	Écrire	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestFailover	Accorde l'autorisation de tester le basculement automatique sur un groupe de nœuds spécifié dans un groupe de réplication.	Écrire	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
TestMigration	Accorde l'autorisation de tester une migration de données depuis Redis hébergé sur Amazon EC2 ElastiCache vers Redis	Écrire	replicationgroup*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon ElastiCache

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> Le nom de la ressource dans la chaîne ARN doit être en minuscules pour être effectif.

Types de ressources	ARN	Clés de condition
parametergroup	`arn:${Partition}:elasticache:${Region}:${Account}:parametergroup:${CacheParameterGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName
securitygroup	`arn:${Partition}:elasticache:${Region}:${Account}:securitygroup:${CacheSecurityGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
subnetgroup	`arn:${Partition}:elasticache:${Region}:${Account}:subnetgroup:${CacheSubnetGroupName}`	aws:RequestTag/${TagKey}

Types de ressources	ARN	Clés de condition
		aws:ResourceTag/${TagKey} aws:TagKeys

Types de ressources	ARN	Clés de condition
replicationgroup	`arn:${Partition}:elasticache:${Region}:${Account}:replicationgroup:${ReplicationGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled

Types de ressources	ARN	Clés de condition
		elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit elasticache:TransitEncryptionEnabled

Types de ressources	ARN	Clés de condition
cluster	arn:${Partition}:elasticache:${Region}:${Account}:cluster:${CacheClusterId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AuthTokenEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:EngineType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:SnapshotRetentionLimit
reserved-instance	arn:${Partition}:elasticache:${Region}:${Account}:reserved-instance:${ReservedCacheNodeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Types de ressources	ARN	Clés de condition
snapshot	arn:${Partition}:elasticache:${Region}:${Account}:snapshot:${SnapshotName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Types de ressources	ARN	Clés de condition
globalreplicationgroup	arn:${Partition}:elasticache::${Account}:globalreplicationgroup:${GlobalReplicationGroupId}	elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit

Types de ressources	ARN	Clés de condition
		elasticache:TransitEncryptionEnabled
user	arn:${Partition}:elasticache:${Region}:${Account}:user:${UserId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode
usergroup	arn:${Partition}:elasticache:${Region}:${Account}:usergroup:${UserGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Types de ressources	ARN	Clés de condition
serverlesscache	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscache:${ServerlessCacheName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:DataStorageUnit elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MaximumDataStorage elasticache:MaximumECPUPerSecond elasticache:MinimumDataStorage elasticache:MinimumECPUPerSecond elasticache:SnapshotRetentionLimit

Types de ressources	ARN	Clés de condition
serverlesscachesnapshot	arn:${Partition}:elasticache:${Region}:${Account}:serverlesscachesnapshot:${ServerlessCacheSnapshotName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Clés de condition pour Amazon ElastiCache

Amazon ElastiCache définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

> **Note**
>
> Pour créer des éléments de condition à l'aide de clés de condition de type chaîne, utilisez les opérateurs de condition qui ne distinguent pas les majuscules des StringNotEqualsIgnoreCase minuscules StringEqualsIgnoreCase ou pour comparer une clé à une valeur de chaîne.
> Pour plus d'informations sur les conditions d'une politique IAM permettant de contrôler l'accès ElastiCache, consultez la section ElastiCache Clés du guide de l' ElastiCache utilisateur Amazon.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction des balises qui sont transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des balises associées à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction des clés de balise qui sont transmises dans la demande	ArrayOfString
elasticache:AtRestEncryptionEnabled	Filtre l'accès en fonction du AtRestEncryptionEnabled paramètre présent dans la demande ou de la valeur fausse par défaut si le paramètre n'est pas présent	Booléen
elasticache:AuthTokenEnabled	Filtre l'accès en fonction de la présence d'un AuthToken paramètre non vide dans la requête	Booléen
elasticache:AutomaticFailoverEnabled	Filtre l'accès en fonction du AutomaticFailoverEnabled paramètre contenu dans la demande	Booléen
elasticache:CacheNodeType	Filtre l'accès en fonction du cacheNodeType paramètre présent dans la demande. Cette clé peut être utilisée pour restreindre les types de nœuds de cache pouvant être utilisés pour la création de cluster ou les opérations de mise à l'échelle.	String
elasticache:CacheParameterGroupName	Filtre l'accès en fonction du CacheParameterGroupName paramètre contenu dans la demande	String

Clés de condition	Description	Type
elasticache:ClusterModeEnabled	Filtre l'accès en fonction du paramètre de mode cluster présent dans la demande. La valeur par défaut pour les créations d'un groupe de nœuds unique (partition) est false (fausse).	Booléen
elasticache:DataStorageUnit	Filtre l'accès par le CacheUsageLimits. DataStorageParamètre .Unit dans la demande CreateServerlessCache et ModifyServerlessCache	String
elasticache:EngineType	Filtre l'accès en fonction du type de moteur présent dans les demandes de création. Pour les créations de groupes de réplication, le moteur par défaut « redis » est utilisé comme clé si le paramètre n'est pas présent	String
elasticache:EngineVersion	Filtre l'accès en fonction du paramètre EngineVersion présent dans les demandes de création ou de modification de cluster.	String
elasticache:KmsKeyId	Filtre l'accès en fonction de l'ID de la clé KMS	String
elasticache:MaximumDataStorage	Filtre l'accès par le CacheUsageLimits. DataStorage.Paramètre maximal dans la demande CreateServerlessCache et ModifyServerlessCache	Numérique
elasticache:MaximumECPUPerSecond	Filtre l'accès par le CacheUsageLimits. ECPUPerDeuxième paramètre maximum dans la demande et CreateServerlessCache ModifyServerlessCache	Numérique
elasticache:MinimumDataStorage	Filtre l'accès par le CacheUsageLimits. DataStorage.Paramètre minimal dans la demande CreateServerlessCache et ModifyServerlessCache	Numérique

Clés de condition	Description	Type
elasticache:MinimumECPUPerSecond	Filtre l'accès par le CacheUsageLimits. ECPUPerDeuxième paramètre minimum dans la demande et CreateServerlessCache ModifyServerlessCache	Numérique
elasticache:MultiAZEnabled	Filtre l'accès en fonction du AZMode paramètre, du AZEnabled multiparamètre ou du nombre de zones de disponibilité dans lesquelles le cluster ou le groupe de réplication peut être placé	Booléen
elasticache:NumNodeGroups	Filtre l'accès en fonction du NodeGroupCount paramètre NumNodeGroups ou spécifié dans la demande. Cette clé peut être utilisée pour restreindre le nombre de groupes de nœuds (partitions) que les clusters peuvent avoir après les opérations de création ou de mise à l'échelle.	Numérique
elasticache:ReplicasPerNodeGroup	Filtre l'accès en fonction du nombre de réplicas par groupe de nœuds (partitions) spécifié dans les créations ou les demandes de mise à l'échelle.	Numérique
elasticache:SnapshotRetentionLimit	Filtre l'accès en fonction du SnapshotRetentionLimit paramètre contenu dans la demande	Numérique
elasticache:TransitEncryptionEnabled	Filtre l'accès en fonction du TransitEncryptionEnabled paramètre présent dans la demande. Pour les créations de groupes de réplication, la valeur par défaut "false" est utilisée comme clé si le paramètre n'est pas présent	Booléen
elasticache:UserAuthenticationMode	Filtre l'accès en fonction du UserAuthenticationMode paramètre contenu dans la demande	String

Actions, ressources et clés de condition pour les appareils et AWS logiciels Elemental

AWS Elemental Appliances and Software (préfixe de service :`elemental-appliances-software`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les appareils et AWS logiciels Elemental
- Types de ressources définis par les appliances et logiciels AWS Elemental
- Clés de condition pour les appareils et logiciels AWS Elemental

Actions définies par les appareils et AWS logiciels Elemental

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CompleteUpload [autorisation uniquement]	Accorde l'autorisation de charger une pièce jointe pour un devis ou une commande	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOrderV1 [autorisation uniquement]	Accorde l'autorisation de créer une ordre.	Écrire			
CreateQuote [autorisation uniquement]	Accorde l'autorisation de créer une requête nommée	Écrire	quote*		
GetAvsCorrectAddress [autorisation uniquement]	Accorde l'autorisation de valider une adresse	Lecture			
GetBillingAddresses [autorisation uniquement]	Accorde l'autorisation de répertorier les adresses de facturation dans le AWS compte	Lecture			
GetDeliveryAddressesV2 [autorisation uniquement]	Accorde l'autorisation de répertorier les adresses de livraison dans le AWS compte	Lecture			
GetOrder [autorisation uniquement]	Accorde l'autorisation de décrire une commande	Lecture			
GetOrdersV2 [autorisation uniquement]	Accorde l'autorisation de répertorier les commandes dans le AWS compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQuote [autorisation uniquement]	Accorde l'autorisation de décrire une requête nommée	Lecture	quote*		
GetTaxes [autorisation uniquement]	Accorde l'autorisation de calculer des taxes pour une commande	Lecture			
ListQuotes [autorisation uniquement]	Accorde l'autorisation de répertorier les devis dans le AWS compte	List			
StartUpload [autorisation uniquement]	Accorde l'autorisation de commencer le chargement d'une pièce jointe pour un devis ou une commande	Écrire			
SubmitOrderV1 [autorisation uniquement]	Accorde l'autorisation de soumettre une commande	Écrire			
UpdateQuote [autorisation uniquement]	Accorde l'autorisation de modifier une requête nommée	Écrire	quote*		

Types de ressources définis par les appliances et logiciels AWS Elemental

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
quote	`arn:${Partition}:elemental-appliances-software:${Region}:${Account}:quote/${ResourceId}`	

Clés de condition pour les appareils et logiciels AWS Elemental

Elemental Appliances and Software ne possède aucune clé de contexte spécifique à un service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les appliances AWS élémentaires et le service d'activation logicielle

AWS Elemental Appliances and Software Activation Service (préfixe de service :`elemental-activations`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les appliances AWS élémentaires et le service d'activation logicielle
- Types de ressources définis par les appliances AWS élémentaires et le service d'activation logicielle

- Clés de condition pour les appliances AWS Elemental et le service d'activation logicielle

Actions définies par les appliances AWS élémentaires et le service d'activation logicielle

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CompleteAccountRegistration [autorisation uniquement]	Accorde l'autorisation de terminer le processus d'enregistrement du compte client pour les achats d'appareils et de logiciels AWS Elemental	Écrire			
CompleteFileUpload [autorisation uniquement]	Accorde l'autorisation de terminer le processus de téléchargement d'un fichier logiciel pour les appareils AWS Elemental et les achats de logiciels	Écrire			
ConfirmAccount [autorisation uniquement]	Accorde l'autorisation de confirmer la propriété des actifs	Écrire			
DownloadKickstart	Autorise le téléchargement des fichiers Kickstart pour	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]	les achats d'appareils et de logiciels AWS Elemental				
DownloadSoftware [autorisation uniquement]	Autorise le téléchargement des fichiers logiciels pour les appareils AWS Elemental et les achats de logiciels	Lecture			
GenerateLicense [autorisation uniquement]	Accorde l'autorisation de générer une licence logicielle pour l'achat d'appareils et de logiciels AWS Elemental	Écrire			
GenerateLicenses [autorisation uniquement]	Autorise la génération de licences logicielles pour les appliances AWS élémentaires et les achats de logiciels	Écrire			
GetArtifactGroupSoftwareVersions [autorisation uniquement]	Accorde l'autorisation de décrire la version logicielle d'un groupe d'artefacts	Lecture			
GetAsset [autorisation uniquement]	Accorde l'autorisation de décrire une ressource	Lecture			
GetAssets [autorisation uniquement]	Accorde l'autorisation de décrire les actifs associés au compte demandeur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProductAdvisories [autorisation uniquement]	Donne l'autorisation d'obtenir tous les avis sur les produits	Lecture			
GetSoftwareVersions [autorisation uniquement]	Accorde l'autorisation de décrire les versions logicielles disponibles	Lecture			
StartFileUpload [autorisation uniquement]	Autorise le lancement du processus de téléchargement d'un fichier logiciel pour les appareils AWS Elemental et les achats de logiciels	Écrire			

Types de ressources définis par les appliances AWS élémentaires et le service d'activation logicielle

AWS Elemental Appliances and Software Activation Service ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès aux appliances AWS élémentaires et au service d'activation logicielle, spécifiez-le `"Resource": "*"` dans votre politique.

Clés de condition pour les appliances AWS Elemental et le service d'activation logicielle

Elemental Activations ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour l' AWS inférence élémentaire

AWS Elemental Inference (préfixe de service :`elemental-inference`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l' AWS inférence élémentaire
- Types de ressources définis par l' AWS inférence élémentaire
- Clés de condition pour l' AWS inférence élémentaire

Actions définies par l' AWS inférence élémentaire

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate Feed	Accorde l'autorisation d'associer un flux à une AWS ressource	Écrire	feed*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFeed	Accorde l'autorisation de créer un nouveau flux	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFeed	Autorise la suppression d'un flux	Écrire	feed*		
DisassociateFeed	Accorde l'autorisation de dissocier un flux d'une ressource AWS	Écrire	feed*		
GetFeed	Accorde l'autorisation d'obtenir les détails du fil	Lecture	feed*		
GetMetadata	Accorde l'autorisation de récupérer des métadonnées pour une sortie de flux spécifique	Lecture	feed*		
ListFeeds	Accorde l'autorisation de répertorier les flux dans le compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises sur une ressource	Lecture			
PutMedia	Autorise le téléchargement de données multimédia pour un flux spécifique	Écrire	feed*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	feed		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	feed		
				aws:TagKeys	
UpdateFeed	Accorde l'autorisation de mettre à jour la configuration du flux	Écrire	feed*		

Types de ressources définis par l' AWS inférence élémentaire

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
feed	`arn:${Partition}:elemental-inference:${Region}:${Account}:feed/${Id}`	aws:ResourceTag/${TagKey}

Clés de condition pour l' AWS inférence élémentaire

AWS L'inférence élémentaire définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elemental MediaConnect

AWS Elemental MediaConnect (préfixe de service :`mediaconnect`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental MediaConnect
- Types de ressources définis par AWS Elemental MediaConnect
- Clés de condition pour AWS Elemental MediaConnect

Actions définies par AWS Elemental MediaConnect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddBridgeOutputs	Octroie l'autorisation d'ajouter des sorties à un pont existant.	Écrire	Bridge*		
AddBridgeSources	Octroie l'autorisation d'ajouter des sources à un pont existant.	Écrire	Bridge*		
AddFlowMediaStreams	Accorde l'autorisation d'ajouter des flux multimédias à n'importe quel flux	Écriture	Flow*		
			MediaStream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
AddFlowOutputs	Accorde l'autorisation d'ajouter des sorties à n'importe quel flux.	Écriture	Flow*		
			Output*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddFlowSources	Accorde l'autorisation d'ajouter des sources à n'importe quel flux.	Écriture	Flow*		
			Source*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddFlowVpcInterfaces	Accorde l'autorisation d'ajouter des interfaces VPC à n'importe quel flux.	Écrire	Flow*		
			VpcInterface*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateRouterNetworkInterface	Accorde l'autorisation d'associer une interface réseau de routeur	Écrire			
CreateBridge	Octroie l'autorisation de créer des ponts.	Écrire	Bridge*		
CreateFlow	Accorde l'autorisation de créer des flux.	Écrire	Flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	Octroie l'autorisation de créer des passerelles.	Écrire	Gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRouterInput	Accorde l'autorisation de créer une nouvelle entrée de routeur dans AWS Elemental MediaConnect	Écrire	RouterInput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:CreateRouterInput mediaconnect:TagResource mediaconnect:UpdateFlowOutput

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouterNetworkInterface	Accorde l'autorisation de créer une nouvelle interface réseau de routeur dans AWS Elemental MediaConnect	Écrire	RouterNetworkInterface*		iam:CreateServiceLinkedRole mediaconnect:CreateRouterNetworkInterface mediaconnect:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRouterOutput	Accorde l'autorisation de créer une nouvelle sortie de routeur dans AWS Elemental MediaConnect	Écrire	RouterOutput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:CreateRouterOutput mediaconnect:TagResource mediaconnect:UpdateFlowSource medialive:UpdateInput

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBridge	Octroie l'autorisation de supprimer des ponts.	Écrire	Bridge*		
DeleteFlow	Accorde l'autorisation de supprimer des flux.	Écrire	Flow*		
DeleteGateway	Octroie l'autorisation de supprimer des passerelles.	Écrire	Gateway*		
DeleteRouterInput	Accorde l'autorisation de supprimer une entrée de routeur dans AWS Elemental MediaConnect	Écrire	RouterInput*		
DeleteRouterNetworkInterface	Accorde l'autorisation de supprimer l'interface réseau d'un routeur dans AWS Elemental MediaConnect	Écrire	RouterNetworkInterface*		
DeleteRouterOutput	Accorde l'autorisation de supprimer une sortie de routeur d' AWS Elemental MediaConnect	Écrire	RouterOutput*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterGatewayInstance	Octroie l'autorisation d'annuler l'enregistrement d'une instance de passerelle.	Écrire	GatewayInstance*		
DescribeBridge	Octroie l'autorisation d'afficher les informations d'un pont.	Lecture	Bridge*		
DescribeFlow	Accorde l'autorisation d'afficher les détails d'un flux, y compris l'ARN, le nom et la zone de disponibilité du flux, ainsi que des détails sur la source, les sorties et les droits.	Lecture	Flow*		
DescribeFlowSourceMetadata	Autorise l'affichage des informations sur le flux de transport source et les programmes du flux	Lecture	Flow*		
DescribeFlowSourceThumbnail	Autorise l'affichage de la miniature de la source du flux	Lecture	Flow*		
DescribeGateway	Octroie l'autorisation d'afficher les informations d'une passerelle, y compris l'ARN, le nom et les blocs d'adresse CIDR de la passerelle, ainsi que des informations sur les réseaux.	Lecture	Gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGatewayInstance	Octroie l'autorisation d'afficher les informations relatives à l'instance d'une passerelle.	Lecture	GatewayInstance*		
DescribeOffering	Accorde l'autorisation d'afficher les informations d'une offre.	Lecture	Offering*		
DescribeReservation	Accorde l'autorisation d'afficher les informations d'une réservation.	Lecture	Reservation*		
DiscoverGatewayPollEndpoint	Octroie l'autorisation de découvrir le point de terminaison d'interrogation de la passerelle.	Lecture	Gateway*		
GetRouterInput	Accorde l'autorisation de récupérer des informations sur une entrée de routeur spécifique dans AWS Elemental MediaConnect	Lecture	RouterInput*		
GetRouterInputSourceMetadata	Accorde l'autorisation de récupérer des métadonnées sur une source d'entrée de routeur dans AWS Elemental MediaConnect	Lecture	RouterInput*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRouterInputThumbnail	Accorde l'autorisation de récupérer la miniature d'une entrée de routeur dans Elemental AWS MediaConnect	Lecture	RouterInput*		
GetRouterNetworkInterface	Accorde l'autorisation de récupérer des informations sur une interface réseau de routeur spécifique dans AWS Elemental MediaConnect	Lecture	RouterNetworkInterface*		
GetRouterOutput	Accorde l'autorisation de récupérer des informations sur une sortie de routeur spécifique dans AWS Elemental MediaConnect	Lecture	RouterOutput*		
GrantFlowEntitlements	Accorde l'autorisation d'accorder des droits sur n'importe quel flux.	Écrire	Entitlement*		
			Flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBridges	Octroie l'autorisation d'afficher une liste des ponts associés à ce compte ainsi qu'à un ARN éventuellement spécifié.	List			
ListEntitlements	Accorde l'autorisation d'afficher la liste de tous les droits qui ont été accordés au compte.	Liste			
ListFlows	Accorde l'autorisation d'afficher la liste des flux qui sont associés à ce compte.	List			
ListGatewayInstances	Octroie l'autorisation d'afficher une liste des instances qui sont associées à cette passerelle.	List			
ListGateways	Octroie l'autorisation d'afficher une liste des passerelles qui sont associées à ce compte.	List			
ListOfferings	Autorise l'affichage d'une liste de toutes les offres disponibles pour le compte en cours Région AWS	List			
ListReservations	Accorde l'autorisation d'afficher une liste de toutes les réservations qui ont été achetées par le compte dans le Région AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRouterInputs	Accorde l'autorisation de récupérer une liste des entrées du routeur dans AWS Elemental MediaConnect	List			
ListRouterNetworkInterfaces	Accorde l'autorisation de récupérer une liste des interfaces réseau des routeurs dans AWS Elemental MediaConnect	List			
ListRouterOutputs	Accorde l'autorisation de récupérer une liste des sorties du routeur dans AWS Elemental MediaConnect	List			
ListTagsForResource	Accorde l'autorisation d'afficher une liste de toutes les balises associées à une ressource.	Lecture			
PollGateway	Octroie l'autorisation d'interroger la passerelle.	Écrire			
PurchaseOffering	Accorde l'autorisation d'acheter une offre.	Écrire	Reservation*		
RemoveBridgeOutput	Octroie l'autorisation de supprimer une sortie d'un pont existant.	Écrire	Bridge*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveBridgeSource	Octroie l'autorisation de supprimer une source d'un pont existant.	Écrire	Bridge*		
RemoveFlowMediaStream	Accorde l'autorisation de supprimer des flux multimédias de n'importe quel flux.	Écriture	Flow*		
			MediaStream*		
RemoveFlowOutput	Accorde l'autorisation de supprimer des sorties de n'importe quel flux.	Écriture	Flow*		
			Output*		
RemoveFlowSource	Accorde l'autorisation de supprimer des sources de n'importe quel flux.	Écriture	Flow*		
			Source*		
RemoveFlowVpcInterface	Accorde l'autorisation de supprimer des interfaces VPC de n'importe quel flux.	Écrire	Flow*		
			VpcInterface*		
RestartRouterInput	Autorise le redémarrage d'une entrée de routeur dans AWS Elemental MediaConnect	Écrire	RouterInput*		
RestartRouterOutput	Autorise le redémarrage d'une sortie de routeur dans AWS Elemental MediaConnect	Écrire	RouterOutput*		
RevokeFlowEntitlement	Accorde l'autorisation de révoquer des droits sur n'importe quel flux.	Écriture	Entitlement*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Flow*		
StartFlow	Accorde l'autorisation de démarrer des flux.	Écrire	Flow*		
StartRouterInput	Accorde l'autorisation de démarrer une entrée de routeur dans AWS Elemental MediaConnect	Écrire	RouterInput*		
StartRouterOutput	Accorde l'autorisation de démarrer une sortie de routeur dans AWS Elemental MediaConnect	Écrire	RouterOutput*		
StopFlow	Accorde l'autorisation d'arrêter des flux.	Écrire	Flow*		
StopRouterInput	Accorde l'autorisation d'arrêter une entrée de routeur dans AWS Elemental MediaConnect	Écrire	RouterInput*		
StopRouterOutput	Accorde l'autorisation d'arrêter la sortie d'un routeur dans AWS Elemental MediaConnect	Écrire	RouterOutput*		
SubmitGatewayStateChange	Octroie l'autorisation de soumettre une modification de l'état de la passerelle.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'associer des balises à des ressources.	Identification	Entitlement		
			Flow		
			MediaStream		
			Output		
			RouterInput		
			RouterNetworkInterface		
			RouterOutput		
			Source		
			VpcInterface		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TakeRouterInput	Accorde l'autorisation d'associer une entrée de routeur à une sortie de routeur dans AWS Elemental MediaConnect	Écrire	RouterOutput*		
UntagResource	Accorde l'autorisation de supprimer des balises des ressources.	Identification	Entitlement		
			Flow		
			MediaStream		
			Output		
			RouterInput		
			RouterNetworkInterface		
			RouterOutput		
			Source		
			VpcInterface		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateBridge	Octroie l'autorisation de mettre à jour des ponts.	Écrire	Bridge*		
UpdateBridgeOutput	Octroie l'autorisation de mettre à jour une sortie d'un pont existant.	Écrire	Bridge*		
UpdateBridgeSource	Octroie l'autorisation de mettre à jour une source d'un pont existant.	Écrire	Bridge*		
UpdateBridgeState	Octroie l'autorisation de mettre à jour l'état d'un pont existant.	Écrire	Bridge*		
UpdateFlow	Accorde l'autorisation de mettre à jour des flux.	Écriture	Flow*		
UpdateFlowEntitlement	Accorde l'autorisation de mettre à jour des droits sur n'importe quel flux.	Écriture	Flow*		
UpdateFlowMediaStream	Accorde l'autorisation de mettre à jour des flux multimédias sur n'importe quel flux.	Écriture	Flow* MediaStream*		
UpdateFlowOutput	Accorde l'autorisation de mettre à jour des sorties sur n'importe quel flux.	Écriture	Flow* Output*		
UpdateFlowSource	Accorde l'autorisation de mettre à jour la source de n'importe quel flux.	Écrire	Flow* Source*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGatewayInstance	Accorde l'autorisation de mettre à jour la configuration d'une instance de passerelle existante	Écrire	GatewayInstance*		
UpdateRouterInput	Accorde l'autorisation de mettre à jour la configuration d'une entrée de routeur dans AWS Elemental MediaConnect	Écrire	RouterInput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:UpdateFlowOutput mediaconnect:UpdateRouterInput

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRouterNetworkInterface	Accorde l'autorisation de mettre à jour la configuration de l'interface réseau d'un routeur dans AWS Elemental MediaConnect	Écrire	RouterNetworkInterface*		iam:CreateServiceLinkedRole mediaconnect:UpdateRouterNetworkInterface

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRouterOutput	Accorde l'autorisation de mettre à jour la configuration d'une sortie de routeur dans AWS Elemental MediaConnect	Écrire	RouterOutput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:UpdateFlowSource mediaconnect:UpdateRouterOutput medialive:UpdateInput

Types de ressources définis par AWS Elemental MediaConnect

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Bridge	`arn:${Partition}:mediaconnect:${Region}:${Account}:bridge:${BridgeId}:${BridgeName}`	
Entitlement	`arn:${Partition}:mediaconnect:${Region}:${Account}:entitlement:${FlowId}:${EntitlementName}`	aws:ResourceTag/${TagKey}
Flow	`arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}`	aws:ResourceTag/${TagKey}
Gateway	`arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}`	
GatewayInstance	`arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}:instance:${InstanceId}`	
MediaStream	`arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}/mediaStream/${MediaStreamName}`	aws:ResourceTag/${TagKey}
Offering	`arn:${Partition}:mediaconnect:${Region}:offering:${OfferingId}`	
Output	`arn:${Partition}:mediaconnect:${Region}:${Account}:output:${OutputId}:${OutputName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Reservation	arn:${Partition}:mediaconnect:${Region}:${Account}:reservation:${ReservationId}:${ReservationName}	
RouterInput	arn:${Partition}:mediaconnect:${Region}:${Account}:routerInput:${RouterInputId}	aws:ResourceTag/${TagKey}
RouterNetworkInterface	arn:${Partition}:mediaconnect:${Region}:${Account}:routerNetworkInterface:${RouterNetworkInterfaceId}	aws:ResourceTag/${TagKey}
RouterOutput	arn:${Partition}:mediaconnect:${Region}:${Account}:routerOutput:${RouterOutputId}	aws:ResourceTag/${TagKey}
Source	arn:${Partition}:mediaconnect:${Region}:${Account}:source:${SourceId}:${SourceName}	aws:ResourceTag/${TagKey}
VpcInterface	arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}/vpcInterface/${VpcInterfaceName}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Elemental MediaConnect

AWS Elemental MediaConnect définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elemental MediaConvert

AWS Elemental MediaConvert (préfixe de service :`mediaconvert`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental MediaConvert
- Types de ressources définis par AWS Elemental MediaConvert
- Clés de condition pour AWS Elemental MediaConvert

Actions définies par AWS Elemental MediaConvert

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate Certificate	Accorde l'autorisation d'associer un Amazon Resource Name (ARN) de AWS Certificate Manager (ACM) à Elemental AWS MediaConvert	Écrire			
CancelJob	Autorise l'annulation d'une MediaConvert tâche AWS élémentaire en attente	Écrire	Job*		
CreateJob	Accorde l'autorisation de créer et de soumettre une AWS tâche élémentaire MediaConvert	Écrire	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys mediaconvert:HttpInputsAllowed mediaconvert:Https	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				InputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	Accorde l'autorisation de créer un AWS modèle de travail MediaConvert personnalisé Elemental	Écrire	Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePreset	Autorise la création d'un AWS préréglage de sortie MediaConvert personnalisé Elemental	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateQueue	Accorde l'autorisation de créer une file d' AWS attente de MediaConvert tâches Elemental	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateResourceShare	Accorde l'autorisation de partager une AWS tâche élémentaire MediaConvert	Écrire	Job		
DeleteJobTemplate	Accorde l'autorisation de supprimer un AWS modèle de travail MediaConvert personnalisé Elemental	Écrire	JobTemplate*		
DeletePolicy	Accorde l'autorisation de supprimer une AWS politique élémentaire MediaConvert	Écrire			
DeletePreset	Autorise la suppression d'un AWS préréglage de sortie MediaConvert personnalisé Elemental	Écrire	Preset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteQueue	Accorde l'autorisation de supprimer une file d' AWS attente de MediaConvert tâches Elemental	Écrire	Queue*		
DescribeEndpoints	Accorde l'autorisation de s'abonner au MediaConvert service AWS Elemental en envoyant une demande pour un point de terminaison spécifique au compte. Toutes les demandes de transcodage doivent être envoyées au point de terminaison renvoyé par le service	List			
DisassociateCertificate	Accorde l'autorisation de supprimer une association entre l'Amazon Resource Name (ARN) d'un AWS certificat Certificate Manager (ACM) et une ressource AWS élémentaire MediaConvert	Écrire			
GetJob	Donne l'autorisation d'obtenir un emploi dans AWS Elemental MediaConvert	Lecture	Job*		
GetJobTemplate	Accorde l'autorisation d'obtenir un modèle de MediaConvert travail AWS Elemental	Lecture	JobTemplate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPolicy	Accorde l'autorisation d'obtenir une AWS politique élémentaire MediaConvert	Lecture			
GetPreset	Accorde l'autorisation d'obtenir un AWS préréglage MediaConvert de sortie élémentaire	Lecture	Preset*		
GetQueue	Accorde l'autorisation d'obtenir une file d' AWS attente de MediaConvert tâches Elemental	Lecture	Queue*		
ListJobTemplates	Accorde l'autorisation de répertorier les modèles de MediaConvert tâches AWS Elemental	List			
ListJobs	Donne l'autorisation de répertorier les AWS emplois élémentaires MediaConvert	List	Queue		
ListPresets	Permet de répertorier les AWS préréglages de MediaConvert sortie élémentaires	List			
ListQueues	Accorde l'autorisation de répertorier les files d'attente de MediaConvert tâches AWS Elemental	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de récupérer les balises MediaConvert d'une file d'attente, d'un préréglage ou d'un modèle de tâche	Lecture	Job		
			JobTemplate		
			Preset		
			Queue		
ListVersions	Accorde l'autorisation de répertorier les versions du moteur de MediaConvert tâches AWS Elemental	List			
Probe	Accorde l'autorisation de sonder un fichier	Lecture			
PutPolicy	Autorise la mise en place d'une AWS politique élémentaire MediaConvert	Écrire			
SearchJobs	Donne l'autorisation de rechercher des emplois dans AWS Elemental MediaConvert	List	Queue		
TagResource	Accorde l'autorisation d'ajouter des balises à une MediaConvert file d'attente, à un préréglage ou à un modèle de tâche	Identification	Job		
			JobTemplate		
			Preset		
			Queue		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises d'une MediaConvert file d'attente, d'un préréglage ou d'un modèle de tâche	Identification	Job		
			JobTemplate		
			Preset		
			Queue		
				aws:TagKeys	
UpdateJobTemplate	Accorde l'autorisation de mettre à jour un AWS modèle de travail MediaConvert personnalisé Elemental	Écrire	JobTemplate*		
			Preset		
			Queue		
UpdatePreset	Autorise la mise à jour d'un AWS préréglage de sortie MediaConvert personnalisé Elemental	Écrire	Preset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateQueue	Accorde l'autorisation de mettre à jour une file d' AWS attente de MediaConvert tâches Elemental	Écrire	Queue*		

Types de ressources définis par AWS Elemental MediaConvert

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Job	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobs/${JobId}`	aws:ResourceTag/${TagKey}
Queue	`arn:${Partition}:mediaconvert:${Region}:${Account}:queues/${QueueName}`	aws:ResourceTag/${TagKey}
Preset	`arn:${Partition}:mediaconvert:${Region}:${Account}:presets/${PresetName}`	aws:ResourceTag/${TagKey}
JobTemplate	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobTemplates/${JobTemplateName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
CertificateAssociation	`arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}`	

Clés de condition pour AWS Elemental MediaConvert

AWS Elemental MediaConvert définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de balise dans la requête.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString
mediaconvert:HttpInputsAllowed	Filtre l'accès par une politique de saisie HTTP présente dans le compte	Booléen
mediaconvert:HttpsInputsAllowed	Filtre l'accès par une politique de saisie HTTPS présente dans le compte	Booléen

Clés de condition	Description	Type
mediaconvert:S3InputsAllowed	Filtre l'accès par une politique de saisie S3 présente dans le compte	Booléen

Actions, ressources et clés de condition pour AWS Elemental MediaLive

AWS Elemental MediaLive (préfixe de service :`medialive`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental MediaLive
- Types de ressources définis par AWS Elemental MediaLive
- Clés de condition pour AWS Elemental MediaLive

Actions définies par AWS Elemental MediaLive

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptInputDeviceTransfer	Accorde l'autorisation d'accepter le transfert d'un appareil d'entrée	Écriture	input-device*		
BatchDelete	Accorde l'autorisation de supprimer des canaux, des entrées, des groupes de sécurité d'entrée et des liaisons multiplex	Écriture			
BatchStart	Accorde l'autorisation de démarrer des canaux et des liaisons multiplex	Écriture			
BatchStop	Accorde l'autorisation d'arrêter des canaux et des liaisons multiplex.	Écriture			
BatchUpdateSchedule	Accorde l'autorisation d'ajouter des actions à la planification d'un canal et de supprimer des actions de cette dernière	Écriture	channel*		
CancelInputDeviceTransfer	Accorde l'autorisation d'annuler le transfert d'un appareil d'entrée	Écrire	input-device*		
ClaimDevice	Accorde l'autorisation de revendiquer un appareil d'entrée	Écrire	input-device*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateChannel	Accorde l'autorisation de créer un canal.	Écrire	channel*		
			input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateChannelPlacementGroup	Accorde l'autorisation de créer un cluster.	Écrire	channel-placement-group*		
			cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplate	Autorise la création d'un modèle d'alarme Cloudwatch	Écrire	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplateGroup	Autorise la création d'un groupe de modèles d'alarmes Cloudwatch	Écrire	cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Accorde l'autorisation de créer un cluster.	Écrire	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplate	Accorde l'autorisation de créer un modèle de règle Eventbridge	Écrire	eventbridge-rule-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplateGroup	Accorde l'autorisation de créer un groupe de modèles de règles Eventbridge	Écrire	eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Accorde l'autorisation de créer une entrée.	Écriture	input*		
			input-security-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInputSecurityGroup	Accorde l'autorisation de créer un groupe de sécurité d'entrée.	Écriture	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplex	Accorde l'autorisation de créer une liaison multiplex	Écriture	multiplex*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplexProgram	Accorde l'autorisation de créer un programme multiplex	Écrire	multiplex*		
CreateNetwork	Accorde l'autorisation de créer un réseau	Écrire	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNode	Accorde l'autorisation de créer un nœud	Écrire	cluster*		
			node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodeRegistrationScript	Accorde l'autorisation de créer un script d'enregistrement de nœud	Écrire	cluster*		
CreatePartnerInput	Accorde l'autorisation de créer une entrée de partenaire	Écrire	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSdiSource	Accorde l'autorisation de créer une source SDI	Écrire	sdi-source*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalMap	Autorise la création d'une carte des signaux	Écrire	signal-map*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Autorise la création de balises pour les canaux, les entrées, les groupes de sécurité d'entrée, les multiplexes, les réservations, les nœuds, les réseaux, les clusters, les groupes de placement des canaux, les cartes de signaux, les sources SDI, les groupes de modèles et les modèles	Identification	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Accorde l'autorisation de supprimer un canal.	Écrire	channel*		
DeleteChannelPlacementGroup	Accorde l'autorisation de supprimer un cluster	Écrire	channel-placement-group*		
DeleteCloudWatchAlarmTemplate	Autorise la suppression d'un modèle d'alarme Cloudwatch	Écrire	cloudwatch-alarm-template*		
DeleteCloudWatchAlarmTemplateGroup	Autorise la suppression d'un groupe de modèles d'alarmes Cloudwatch	Écrire	cloudwatch-alarm-template-group*		
DeleteCluster	Accorde l'autorisation de supprimer un cluster	Écrire	cluster*		
DeleteEventBridgeRuleTemplate	Accorde l'autorisation de supprimer un modèle de règle Eventbridge	Écrire	eventbridge-rule-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEventBridgeRuleTemplateGroup	Accorde l'autorisation de supprimer un groupe de modèles de règles Eventbridge	Écrire	eventbridge-rule-template-group*		
DeleteInput	Accorde l'autorisation de supprimer une entrée.	Écriture	input*		
DeleteInputSecurityGroup	Accorde l'autorisation de supprimer un groupe de sécurité d'entrée.	Écriture	input-security-group*		
DeleteMultiplex	Accorde l'autorisation de supprimer une liaison multiplex	Écriture	multiplex*		
DeleteMultiplexProgram	Accorde l'autorisation de supprimer un programme multiplex	Écrire	multiplex*		
DeleteNetwork	Accorde l'autorisation de supprimer un réseau	Écrire	network*		
DeleteNode	Accorde l'autorisation de supprimer un nœud	Écrire	node*		
DeleteReservation	Accorde l'autorisation de supprimer une réservation expirée.	Écriture	reservation*		
DeleteSchedule	Accorde l'autorisation de supprimer toutes les actions de planification pour un canal	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSdiSource	Accorde l'autorisation de supprimer une source SDI	Écrire	sdi-source*		
DeleteSignalMap	Autorise la suppression d'une carte de signalisation	Écrire	signal-map*		
DeleteTags	Autorise la suppression des balises des canaux, des entrées, des groupes de sécurité d'entrée, des multiplexes, des réservations, des nœuds, des clusters, des réseaux, des groupes de placement des canaux, des sources SDI, des cartes de signaux, des groupes de modèles et des modèles	Identification	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
				aws:TagKeys	
DescribeAccountConfiguration	Octroie l'autorisation d'afficher la configuration du compte du client.	Lecture			
DescribeChannel	Accorde l'autorisation d'obtenir des détails sur un canal.	Lecture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeChannelPlacementGroup	Autorise à décrire un groupe de placement de chaînes	Lecture	channel-placement-group*		
DescribeCluster	Accorde l'autorisation de décrire un cluster	Lecture	cluster*		
DescribeInput	Accorde l'autorisation de décrire une entrée.	Lecture	input*		
DescribeInputDevice	Accorde l'autorisation de décrire un appareil d'entrée.	Lecture	input-device*		
DescribeInputDeviceThumbnail	Accorde l'autorisation de décrire la vignette d'un appareil d'entrée	Lecture	input-device*		
DescribeInputSecurityGroup	Accorde l'autorisation de décrire un groupe de sécurité d'entrée.	Lecture	input-security-group*		
DescribeMultiplex	Accorde l'autorisation de décrire une liaison multiplex	Lecture	multiplex*		
DescribeMultiplexProgram	Accorde l'autorisation de décrire un programme multiplex	Lecture	multiplex*		
DescribeNetwork	Accorde l'autorisation de décrire un réseau	Lecture	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeNode	Accorde l'autorisation de décrire un nœud	Lecture	node*		
DescribeOffering	Accorde l'autorisation d'obtenir des détails sur une offre de réservation.	Lecture	offering*		
DescribeReservation	Accorde l'autorisation d'obtenir des détails sur une réservation.	Lecture	reservation*		
DescribeSchedule	Accorde l'autorisation d'afficher la liste des actions planifiées sur un canal	Lecture	channel*		
DescribeSdiSource	Autorise la description d'une source SDI	Lecture	sdi-source*		
DescribeThumbnails	Octroie l'autorisation d'afficher les miniatures d'une chaîne.	Lecture	channel*		
GetCloudWatchAlarmTemplate	Accorde l'autorisation d'obtenir un modèle d'alarme Cloudwatch	Lecture	cloudwatch-alarm-template*		
GetCloudWatchAlarmTemplateGroup	Accorde l'autorisation d'obtenir un groupe de modèles d'alarmes Cloudwatch	Lecture	cloudwatch-alarm-template-group*		
GetEventBridgeRuleTemplate	Accorde l'autorisation d'obtenir un modèle de règle Eventbridge	Lecture	eventbridge-rule-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEventBridgeRuleTemplateGroup	Accorde l'autorisation d'obtenir un groupe de modèles de règles Eventbridge	Lecture	eventbridge-rule-template-group*		
GetSignalMap	Autorise l'obtention d'une carte de signalisation	Lecture	signal-map*		
ListAlerts	Accorde l'autorisation de répertorier les alertes des chaînes	List			
ListChannelPlacementGroups	Accorde l'autorisation de répertorier les groupes de placement de chaînes	List			
ListChannels	Accorde l'autorisation de répertorier les canaux.	List			
ListCloudWatchAlarmTemplateGroups	Autorise à répertorier les groupes de modèles d'alarmes Cloudwatch	List			
ListCloudWatchAlarmTemplates	Accorde l'autorisation de répertorier les modèles d'alarmes Cloudwatch	List			
ListClusterAlerts	Accorde l'autorisation de répertorier les alertes du cluster	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListClusters	Accorde l'autorisation de répertorier les clusters virtuels	List			
ListEventBridgeRuleTemplateGroups	Accorde l'autorisation de répertorier les groupes de modèles de règles Eventbridge	List			
ListEventBridgeRuleTemplates	Accorde l'autorisation de répertorier les modèles de règles Eventbridge	List			
ListInputDeviceTransfers	Accorde l'autorisation de répertorier les transferts des appareils d'entrée	Liste			
ListInputDevices	Accorde l'autorisation de répertorier les appareils d'entrée.	Liste			
ListInputSecurityGroups	Accorde l'autorisation de répertorier les groupes de sécurité d'entrée.	Liste			
ListInputs	Accorde l'autorisation de répertorier les entrées.	List			
ListMultiplexAlerts	Accorde l'autorisation de répertorier les alertes multiplex	List			
ListMultiplexPrograms	Accorde l'autorisation de répertorier les programmes multiplex	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMultiplexes	Accorde l'autorisation de répertorier les liaisons multiplex	List			
ListNetworks	Accorde l'autorisation de répertorier les réseaux	List			
ListNodes	Accorde l'autorisation de répertorier les nœuds	List			
ListOfferings	Accorde l'autorisation de répertorier les offres de réservation.	Liste			
ListReservations	Accorde l'autorisation de répertorier les réservations.	List			
ListSdiSources	Accorde l'autorisation de répertorier les sources SDI	List			
ListSignalMaps	Autorise à répertorier les cartes de signalisation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Permet de répertorier les balises pour les canaux, les entrées, les groupes de sécurité d'entrée, les multiplexes, les réservations, les nœuds, les clusters, les réseaux, les groupes de placement des canaux, les sources SDI, les cartes de signaux, les groupes de modèles et les modèles	List	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
ListVersions	Accorde l'autorisation de répertorier les versions disponibles de MediaLive	List			
PollAnywhere	Autorise le nœud à interroger le cluster	Écrire			
PurchaseOffering	Accorde l'autorisation d'acheter une offre de réservation.	Écrire	offering*		
			reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RebootInputDevice	Accorde l'autorisation de redémarrer un appareil d'entrée	Écrire	input-device*		
RejectInputDeviceTransfer	Accorde l'autorisation de rejeter le transfert d'un appareil d'entrée	Écrire	input-device*		
RestartChannelPipelines	Autorise le redémarrage des pipelines sur un canal actif	Écrire	channel*		
StartChannel	Accorde l'autorisation de démarrer un canal.	Écrire	channel*		
StartDeleteMonitorDeployment	Autorise le lancement de la suppression du moniteur d'une carte des signaux	Écrire	signal-map*		
StartInputDevice	Accorde l'autorisation de démarrer un périphérique d'entrée attaché à un MediaConnect flux	Écrire	input-device*		
StartInputDeviceMaintenanceWindow	Accorde l'autorisation de démarrer une fenêtre de maintenance pour un appareil d'entrée	Écrire	input-device*		
StartMonitorDeployment	Accorde l'autorisation de démarrer le déploiement d'un moniteur de carte des signaux	Écrire	signal-map*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMultiplex	Accorde l'autorisation de démarrer une liaison multiplex	Écrire	multiplex*		
StartUpdateSignalMap	Autorise le lancement d'une mise à jour de la carte des signaux	Écrire	signal-map*		
StopChannel	Accorde l'autorisation d'arrêter un canal.	Écrire	channel*		
StopInputDevice	Accorde l'autorisation d'arrêter un périphérique d'entrée attaché à un MediaConnect flux	Écrire	input-device*		
StopMultiplex	Accorde l'autorisation d'arrêter une liaison multiplex	Écrire	multiplex*		
SubmitAnywhereStateChange	Autorise le nœud à soumettre des modifications d'état au cluster	Écrire			
TransferInputDevice	Accorde l'autorisation de transférer un appareil d'entrée	Écrire	input-device*		
UpdateAccountConfiguration	Octroie l'autorisation de mettre à jour la configuration du compte d'un client.	Écrire			
UpdateChannel	Accorde l'autorisation de mettre à jour un canal.	Écriture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateChannelClass	Accorde l'autorisation de mettre à jour la classe d'un canal.	Écrire	channel*		
UpdateChannelPlacementGroup	Accorde l'autorisation de mettre à jour un nœud	Écrire	channel-placement-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateCloudWatchAlarmTemplate	Autorise la mise à jour d'un modèle d'alarme Cloudwatch	Écrire	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
UpdateCloudWatchAlarmTemplateGroup	Autorise la mise à jour d'un groupe de modèles d'alarmes Cloudwatch	Écrire	cloudwatch-alarm-template-group*		
UpdateCluster	Accorde l'autorisation de mettre à jour un cluster	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEventBridgeRuleTemplate	Autorise la mise à jour d'un modèle de règle Eventbridge	Écrire	eventbridge-rule-template*		
			eventbridge-rule-template-group*		
UpdateEventBridgeRuleTemplateGroup	Autorise la mise à jour d'un groupe de modèles de règles Eventbridge	Écrire	eventbridge-rule-template-group*		
UpdateInput	Accorde l'autorisation de mettre à jour une entrée.	Écriture	input*		
UpdateInputDevice	Accorde l'autorisation de mettre à jour un appareil d'entrée.	Écriture	input-device*		
UpdateInputSecurityGroup	Accorde l'autorisation de mettre à jour un groupe de sécurité d'entrée.	Écriture	input-security-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMultiplex	Accorde l'autorisation de mettre à jour une liaison multiplex	Écriture	multiplex*		
UpdateMultiplexProgram	Accorde l'autorisation de mettre à jour un programme multiplex	Écrire	multiplex*		
UpdateNetwork	Accorde l'autorisation de mettre à jour l'état d'un nœud	Écrire	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNode	Accorde l'autorisation de mettre à jour un nœud	Écrire	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNodeState	Accorde l'autorisation de mettre à jour l'état d'un nœud	Écrire	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateReservation	Accorde l'autorisation de mettre à jour une réservation.	Écrire	reservation*		
UpdateSdiSource	Autorise la mise à jour de l'état d'une source SDI	Écrire	sdi-source*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Types de ressources définis par AWS Elemental MediaLive

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
channel	arn:${Partition}:medialive:${Region}:${Account}:channel:${ChannelId}	aws:ResourceTag/${TagKey}
input	arn:${Partition}:medialive:${Region}:${Account}:input:${InputId}	aws:ResourceTag/${TagKey}
input-device	arn:${Partition}:medialive:${Region}:${Account}:inputDevice:${DeviceId}	
input-security-group	arn:${Partition}:medialive:${Region}:${Account}:inputSecurityGroup:${InputSecurityGroupId}	aws:ResourceTag/${TagKey}
multiplex	arn:${Partition}:medialive:${Region}:${Account}:multiplex:${MultiplexId}	aws:ResourceTag/${TagKey}
reservation	arn:${Partition}:medialive:${Region}:${Account}:reservation:${ReservationId}	aws:ResourceTag/${TagKey}
offering	arn:${Partition}:medialive:${Region}:${Account}:offering:${OfferingId}	
signal-map	arn:${Partition}:medialive:${Region}:${Account}:signal-map:${SignalMapId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template-group	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template-group:${CloudWatchAlarmTemplateGroupId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template:${CloudWatchAlarmTemplateId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
eventbridge-rule-template-group	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template-group:${EventBridgeRuleTemplateGroupId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template:${EventBridgeRuleTemplateId}	aws:ResourceTag/${TagKey}
cluster	arn:${Partition}:medialive:${Region}:${Account}:cluster:${ClusterId}	aws:ResourceTag/${TagKey}
node	arn:${Partition}:medialive:${Region}:${Account}:node:${ClusterId}/${NodeId}	aws:ResourceTag/${TagKey}
network	arn:${Partition}:medialive:${Region}:${Account}:network:${NetworkId}	aws:ResourceTag/${TagKey}
channel-placement-group	arn:${Partition}:medialive:${Region}:${Account}:channelPlacementGroup:${ClusterId}/${ChannelPlacementGroupId}	aws:ResourceTag/${TagKey}
sdi-source	arn:${Partition}:medialive:${Region}:${Account}:sdiSource:${SdiSourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Elemental MediaLive

AWS Elemental MediaLive définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elemental MediaPackage

AWS Elemental MediaPackage (préfixe de service :`mediapackage`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental MediaPackage
- Types de ressources définis par AWS Elemental MediaPackage
- Clés de condition pour AWS Elemental MediaPackage

Actions définies par AWS Elemental MediaPackage

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConfigureLogs	Accorde l'autorisation de configurer les journaux d'accès pour un canal	Écrire	channels*		iam:CreateServiceLinkedRole
CreateChannel	Accorde l'autorisation de créer une chaîne dans AWS Elemental MediaPackage	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Autorise la création d'une tâche de récolte dans AWS Elemental MediaPackage	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Accorde l'autorisation de créer un point de terminaison dans AWS Elemental MediaPackage	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteChannel	Autorise la suppression d'une chaîne dans AWS Elemental MediaPackage	Écrire	channels*		
DeleteOriginEndpoint	Accorde l'autorisation de supprimer un point de terminaison dans AWS Elemental MediaPackage	Écrire	origin_endpoints*		
DescribeChannel	Autorise l'affichage des détails d'une chaîne dans AWS Elemental MediaPackage	Lecture	channels*		
DescribeHarvestJob	Accorde l'autorisation de consulter les détails d'une tâche de récolte dans AWS Elemental MediaPackage	Lecture	harvest_jobs*		
DescribeOriginEndpoint	Autorise l'affichage des détails d'un point de terminaison dans AWS Elemental MediaPackage	Lecture	origin_endpoints*		
ListChannels	Autorise l'affichage d'une liste de chaînes dans AWS Elemental MediaPackage	Lecture			
ListHarvestJobs	Permet de consulter une liste des tâches de récolte dans AWS Elemental MediaPackage	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOriginEndpoints	Autorise l'affichage d'une liste de points de terminaison dans Elemental AWS MediaPackage	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les tags assignés à une chaîne ou OriginEndpoint	Lecture	channels		
			harvest_jobs		
			origin_endpoints		
RotateChannelCredentials	Autorise la rotation des informations d'identification pour le premier IngestEndpoint canal dans AWS Elemental MediaPackage	Écrire	channels*		
RotateIngestEndpointCredentials	Autorise la rotation des IngestEndpoint informations d'identification pour une chaîne dans AWS Elemental MediaPackage	Écrire	channels*		
TagResource	Accorde l'autorisation de baliser une MediaPackage ressource	Identification	channels		
			harvest_jobs		
			origin_endpoints		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les tags d'une chaîne ou OriginEndpoint	Identification	channels		
			harvest_jobs		
			origin_endpoints		
				aws:TagKeys	
UpdateChannel	Accorde l'autorisation d'apporter des modifications à une chaîne dans AWS Elemental MediaPackage	Écrire	channels*		
UpdateOriginEndpoint	Accorde l'autorisation d'apporter des modifications à un point de terminaison dans AWS Elemental MediaPackage	Écrire	origin_endpoints*		

Types de ressources définis par AWS Elemental MediaPackage

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
channels	`arn:${Partition}:mediapackage:${Region}:${Account}:channels/${ChannelIdentifier}`	aws:ResourceTag/${TagKey}
origin_endpoints	`arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${OriginEndpointIdentifier}`	aws:ResourceTag/${TagKey}
harvest_jobs	`arn:${Partition}:mediapackage:${Region}:${Account}:harvest_jobs/${HarvestJobIdentifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Elemental MediaPackage

AWS Elemental MediaPackage définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès par tag pour une MediaPackage demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès par balise pour une MediaPackage ressource	String
aws:TagKeys	Filtre l'accès par les clés de balise pour une MediaPackage ressource ou une demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elemental V2 MediaPackage

AWS Elemental MediaPackage V2 (préfixe de service :`mediapackagev2`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental V2 MediaPackage
- Types de ressources définis par AWS Elemental V2 MediaPackage
- Clés de condition pour AWS Elemental V2 MediaPackage

Actions définies par AWS Elemental V2 MediaPackage

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelHarvestJob	Autorise l'annulation d'une tâche de récolte	Écrire	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
CreateChannel	Accorde l'autorisation de créer un canal dans un groupe de canaux.	Écrire	Channel*		
			ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateChannelGroup	Accorde l'autorisation de créer un groupe de canaux.	Écrire	ChannelGroup*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateHarvestJob	Donne l'autorisation de créer un emploi dans le secteur de la récolte	Écrire	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Accorde l'autorisation de créer un point de terminaison d'origine pour un canal.	Écrire	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Accorde l'autorisation de supprimer un canal dans un groupe de canaux.	Écrire	Channel*		
			ChannelGroup*		
DeleteChannelGroup	Accorde l'autorisation de supprimer un groupe de canaux.	Écrire	ChannelGroup*		
DeleteChannelPolicy	Accorde l'autorisation de supprimer une stratégie de ressources d'un canal.	Écrire	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
DeleteOriginEndpoint	Accorde l'autorisation de supprimer un point de terminaison d'origine d'un canal.	Écrire	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteOriginEndpointPolicy	Accorde l'autorisation de supprimer une stratégie de ressources d'un point de terminaison d'origine.	Écrire	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
GetChannel	Accorde l'autorisation de récupérer les détails d'un canal dans un groupe de canaux.	Lecture	Channel*		
			ChannelGroup*		
GetChannelGroup	Accorde l'autorisation de récupérer les détails d'un groupe de canaux.	Lecture	ChannelGroup*		
GetChannelPolicy	Accorde l'autorisation de récupérer une stratégie de ressources pour un canal.	Lecture	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
GetHarvestJob	Permet de récupérer les détails d'une tâche de récolte	Lecture	Channel*		
			ChannelGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			HarvestJob*		
			OriginEndpoint*		
GetHeadObject	Accorde l'autorisation de faire GetHeadObject des demandes à MediaPackage	Lecture	OriginEndpoint*		
GetObject	Accorde l'autorisation de faire GetObject des demandes à MediaPackage	Lecture	OriginEndpoint*		
GetOriginEndpoint	Accorde l'autorisation de récupérer les détails d'un point de terminaison d'origine.	Lecture	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
GetOriginEndpointPolicy	Accorde l'autorisation de récupérer les détails d'une stratégie de ressources pour un point de terminaison d'origine.	Lecture	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
HarvestObject	Accorde l'autorisation de faire HarvestObject des demandes à MediaPackage	Lecture	OriginEndpoint*		
ListChannelGroups	Accorde l'autorisation de répertorier tous les groupes de canaux pour un compte aws.	List			
ListChannels	Accorde l'autorisation de répertorier tous les canaux dans un groupe de canaux.	List	ChannelGroup*		
ListHarvestJobs	Permet de répertorier toutes les tâches de récolte dans un groupe de canaux, un canal, un point de terminaison d'origine	List	ChannelGroup*		
ListOriginEndpoints	Accorde l'autorisation de répertorier tous les points de terminaison d'origine d'un canal.	List	Channel*		
			ChannelGroup*		
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée.	Lecture	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutChannelPolicy	Accorde l'autorisation d'attacher une stratégie de ressources d'un canal.	Écrire	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
PutObject	Accorde l'autorisation de faire PutObject des demandes à MediaPackage	Écrire	Channel*		
PutOriginEndpointPolicy	Accorde l'autorisation d'attacher une stratégie de ressources à un point de terminaison d'origine.	Écrire	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
ResetChannelState	Autorise la réinitialisation d'une chaîne	Écrire	Channel*		
			ChannelGroup*		
ResetOriginEndpointState	Accorde l'autorisation de réinitialiser un point de terminaison d'origine	Écrire	Channel*		
			ChannelGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			OriginEndpoint*		
TagResource	Accorde l'autorisation d'ajouter des balises spécifiées à la ressource spécifiée.	Identification	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de la ressource spécifiée	Identification	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateChannel	Accorde l'autorisation de mettre à jour un canal dans un groupe de canaux.	Écrire	Channel*		
			ChannelGroup*		
UpdateChannelGroup	Accorde l'autorisation de mettre à jour un groupe de canaux.	Écrire	ChannelGroup*		
UpdateOriginEndpoint	Accorde l'autorisation de mettre à jour un point de terminaison d'origine d'un canal.	Écrire	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Types de ressources définis par AWS Elemental V2 MediaPackage

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
ChannelGroup	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}`	aws:ResourceTag/${TagKey}
ChannelPolicy	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}`	
Channel	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}`	aws:ResourceTag/${TagKey}
OriginEndpointPolicy	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}`	
OriginEndpoint	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}`	aws:ResourceTag/${TagKey}
HarvestJob	`arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}/harvestJob/${HarvestJobName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Elemental V2 MediaPackage

AWS Elemental MediaPackage V2 définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les

conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elemental VOD MediaPackage

AWS Elemental MediaPackage VOD (préfixe de service :`mediapackage-vod`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental VOD MediaPackage
- Types de ressources définis par AWS Elemental VOD MediaPackage
- Clés de condition pour AWS Elemental VOD MediaPackage

Actions définies par AWS Elemental VOD MediaPackage

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConfigureLogs	Accorde l'autorisation de configurer les journaux d'accès de sortie pour un PackagingGroup	Écrire	packaging-groups*		iam:CreateServiceLinkedRole
CreateAsset	Accorde l'autorisation de créer un actif dans AWS Elemental MediaPackage	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingConfiguration	Accorde l'autorisation de créer une configuration d'empaquetage dans AWS Elemental MediaPackage	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingGroup	Accorde l'autorisation de créer un groupe d'emballages dans AWS Elemental MediaPackage	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAsset	Accorde l'autorisation de supprimer un actif dans AWS Elemental MediaPackage	Écrire	assets*		
DeletePackagingConfiguration	Accorde l'autorisation de supprimer une configuration d'empaquetage dans AWS Elemental MediaPackage	Écrire	packaging-configurations*		
DeletePackagingGroup	Accorde l'autorisation de supprimer un groupe d'emballages dans AWS Elemental MediaPackage	Écrire	packaging-groups*		
DescribeAsset	Autorise l'affichage des détails d'un actif dans AWS Elemental MediaPackage	Lecture	assets*		
DescribePackagingConfiguration	Accorde l'autorisation d'afficher les détails d'une configuration d'emballage dans AWS Elemental MediaPackage	Lecture	packaging-configurations*		
DescribePackagingGroup	Autorise l'affichage des détails d'un groupe de packaging dans AWS Elemental MediaPackage	Lecture	packaging-groups*		
ListAssets	Autorise l'affichage d'une liste de ressources dans AWS Elemental MediaPackage	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPackagingConfigurations	Autorise l'affichage d'une liste de configurations d'emballage dans AWS Elemental MediaPackage	List			
ListPackagingGroups	Autorise l'affichage d'une liste de groupes d'emballages dans AWS Elemental MediaPackage	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises attribuées à un Packaging Group PackagingConfiguration, ou à un actif	Lecture	assets		
			packaging-configurations		
			packaging-groups		
TagResource	Accorde l'autorisation d'attribuer des balises à un Packaging Group PackagingConfiguration, ou à un actif	Identification	assets		
			packaging-configurations		
			packaging-groups		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises d'une PackagingGroup ressource ou PackagingConfiguration d'une ressource	Identification	assets		
			packaging-configurations		
			packaging-groups		
				aws:TagKeys	
UpdatePackagingGroup	Autorise la mise à jour d'un groupe de packaging dans AWS Elemental MediaPackage	Écrire	packaging-groups*		

Types de ressources définis par AWS Elemental VOD MediaPackage

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
assets	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:assets/${AssetIdentifier}`	aws:ResourceTag/${TagKey}
packaging-configurations	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-configurations/${PackagingConfigurationIdentifier}`	aws:ResourceTag/${TagKey}
packaging-groups	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-groups/${PackagingGroupIdentifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Elemental VOD MediaPackage

AWS Elemental MediaPackage VOD définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elemental MediaStore

AWS Elemental MediaStore (préfixe de service :`mediastore`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental MediaStore
- Types de ressources définis par AWS Elemental MediaStore
- Clés de condition pour AWS Elemental MediaStore

Actions définies par AWS Elemental MediaStore

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateContainer	Accorde l'autorisation de créer un conteneur	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteContainer	Accorde l'autorisation de supprimer un conteneur	Écrire	container*		
DeleteContainerPolicy	Accorde l'autorisation de supprimer la stratégie d'accès d'un conteneur	Gestion des autorisations	container*		
DeleteCorsPolicy	Accorde l'autorisation de supprimer la politique CORS d'un conteneur	Écrire	container*		
DeleteLifecyclePolicy	Accorde l'autorisation de supprimer la politique de cycle de vie d'un conteneur	Écrire	container*		
DeleteMetricPolicy	Accorde l'autorisation de supprimer la politique de métrique d'un conteneur	Écrire	container*		
DeleteObject	Accorde l'autorisation de supprimer un objet	Écrire	object*		
DescribeContainer	Accorde l'autorisation de récupérer des détails sur un conteneur	List	container*		
DescribeObject	Accorde l'autorisation de récupérer les métadonnées d'un objet	List	object*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContainerPolicy	Accorde l'autorisation de récupérer la stratégie d'accès d'un conteneur	Lecture	container*		
GetCorsPolicy	Accorde l'autorisation de récupérer la politique CORS d'un conteneur	Lecture	container*		
GetLifecyclePolicy	Accorde l'autorisation de récupérer la politique de cycle de vie affectée à un conteneur	Lecture	container*		
GetMetricPolicy	Accorde l'autorisation de récupérer la politique de métrique affectée à un conteneur	Lecture	container*		
GetObject	Accorde l'autorisation de récupérer un objet	Lecture	object*		
ListContainers	Accorde l'autorisation de récupérer la liste des conteneurs dans le compte actuel	List			
ListItems	Accorde l'autorisation de récupérer la liste d'objets et de sous-dossiers stockés dans un dossier	List	folder		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les étiquettes sur un conteneur	Lecture	container		
PutContainerPolicy	Accorde l'autorisation de créer ou de remplacer la stratégie d'accès d'un conteneur	Gestion des autorisations	container*		
PutCorsPolicy	Accorde l'autorisation d'ajouter ou de modifier la politique CORS d'un conteneur	Écrire	container*		
PutLifecyclePolicy	Accorde l'autorisation d'ajouter ou de modifier la politique de cycle de vie affectée à un conteneur	Écrire	container*		
PutMetricPolicy	Accorde l'autorisation d'ajouter ou de modifier la politique de métrique affectée à un conteneur	Écrire	container*		
PutObject	Accorde l'autorisation de charger un objet	Écrire	object*		
StartAccessLogging	Accorde l'autorisation de démarrer la journalisation des accès sur un conteneur	Écrire	container*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopAccessLogging	Accorde l'autorisation d'arrêter la journalisation des accès sur un conteneur	Écrire	container *		
TagResource	Accorde l'autorisation d'ajouter des étiquettes à un conteneur	Identification	container		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les étiquettes d'un conteneur	Identification	container		
				aws:TagKeys	

Types de ressources définis par AWS Elemental MediaStore

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
container	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}`	aws:ResourceTag/${TagKey}
object	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${ObjectPath}`	
folder	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${FolderPath}`	

Clés de condition pour AWS Elemental MediaStore

AWS Elemental MediaStore définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Elemental MediaTailor

AWS Elemental MediaTailor (préfixe de service :`mediatailor`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental MediaTailor
- Types de ressources définis par AWS Elemental MediaTailor
- Clés de condition pour AWS Elemental MediaTailor

Actions définies par AWS Elemental MediaTailor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConfigureLogsForChannel	Accorde l'autorisation de lancer le canal avec le nom du canal spécifié	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConfigureLogsForPlaybackConfiguration	Accorde l'autorisation de configurer les journaux pour une configuration de lecture	Écrire	playbackConfiguration*		iam:CreateServiceLinkedRole
CreateChannel	Accorde l'autorisation de créer un canal	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLiveSource	Accorde l'autorisation de créer une source en direct sur l'emplacement source avec le nom de l'emplacement source spécifié	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrefetchSchedule	Accorde l'autorisation de créer une planification de prélecture pour la configuration de lecture avec le nom de configuration de lecture spécifié	Écrire	playbackConfiguration*		
CreateProgram	Accorde l'autorisation de créer un programme sur le canal avec le nom de canal spécifié	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSourceLocation	Accorde l'autorisation de créer un emplacement source	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVodSource	Accorde l'autorisation de créer une source VOD sur l'emplacement source avec le nom de l'emplacement source spécifié	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Accorde l'autorisation de supprimer le canal avec le nom du canal spécifié	Écrire	channel*		
DeleteChannelPolicy	Accorde l'autorisation de supprimer la politique IAM sur le canal avec le nom de canal spécifié	Gestion des autorisations	channel*		
DeleteLiveSource	Accorde l'autorisation de supprimer la source en direct avec le nom de source en direct spécifié sur l'emplacement source avec le nom de l'emplacement source spécifié	Écrire	liveSource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePlaybackConfiguration	Accorde l'autorisation de supprimer la configuration de lecture spécifiée	Écrire	playbackConfiguration*		
DeletePrefetchSchedule	Accorde l'autorisation de supprimer une planification de prélecture pour une configuration de lecture avec le nom de planification de prélecture spécifié	Écrire	playbackConfiguration*		
			prefetchSchedule*		
DeleteProgram	Accorde l'autorisation de supprimer le programme avec le nom de programme spécifié sur le canal avec le nom de canal spécifié	Écrire	program*		
DeleteSourceLocation	Accorde l'autorisation de supprimer l'emplacement source avec le nom de l'emplacement source spécifié	Écrire	sourceLocation*		
DeleteVodSource	Accorde l'autorisation de supprimer la source VOD avec le nom de source VOD spécifié sur l'emplacement source avec le nom de l'emplacement source spécifié	Écrire	vodSource*		
DescribeChannel	Accorde l'autorisation de récupérer le canal avec le nom de canal spécifié	Lecture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeLiveSource	Accorde l'autorisation de récupérer la source en direct avec le nom de source en direct spécifié sur l'emplacement source avec le nom de l'emplacement source spécifié	Lecture	liveSource*		
DescribeProgram	Accorde l'autorisation de récupérer le programme avec le nom de programme spécifié sur le canal avec le nom de canal spécifié	Lecture	program*		
DescribeSourceLocation	Accorde l'autorisation de récupérer l'emplacement source avec le nom de l'emplacement source spécifié	Lecture	sourceLocation*		
DescribeVodSource	Accorde l'autorisation de récupérer la source VOD avec le nom de source VOD spécifié sur l'emplacement source avec le nom de l'emplacement source spécifié	Lecture	vodSource*		
GetChannelPolicy	Accorde l'autorisation de lire la politique IAM sur le canal avec le nom de canal spécifié	Lecture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetChannelSchedule	Accorde l'autorisation de récupérer la planification des programmes sur le canal avec le nom de canal spécifié	Lecture	channel*		
GetPlaybackConfiguration	Accorde l'autorisation de récupérer la configuration pour le nom spécifié.	Lecture	playbackConfiguration*		
GetPrefetchSchedule	Accorde l'autorisation de récupérer la planification de prélecture pour une configuration de lecture avec le nom de planification de prélecture spécifié	Lecture	playbackConfiguration* prefetchSchedule*		
ListAlerts	Accorde l'autorisation de récupérer une liste des alertes sur une ressource	Lecture			
ListChannels	Accorde l'autorisation de récupérer la liste des canaux existants	Lecture			
ListLiveSources	Accorde l'autorisation de récupérer la liste des sources en direct existantes sur l'emplacement source avec le nom de l'emplacement source spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPlaybackConfigurations	Accorde l'autorisation de récupérer la liste des configurations disponibles.	List			
ListPrefetchSchedules	Accorde l'autorisation de récupérer la liste des planifications de prélecture pour une configuration de lecture	List	playbackConfiguration*		
ListSourceLocations	Accorde l'autorisation de récupérer la liste des emplacements sources existants	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications attribuées à la ressource de configuration de lecture spécifiée	Lecture	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
ListVodSources	Accorde l'autorisation de récupérer la liste des sources VOD existantes sur l'emplacement source avec le nom de l'emplacement source spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutChannelPolicy	Accorde l'autorisation de définir la politique IAM sur le canal avec le nom de canal spécifié	Gestion des autorisations	channel*		
PutPlaybackConfiguration	Accorde l'autorisation d'ajouter une nouvelle configuration.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
StartChannel	Accorde l'autorisation de lancer le canal avec le nom du canal spécifié	Écrire	channel*		
StopChannel	Accorde l'autorisation d'arrêter le canal avec le nom du canal spécifié	Écrire	channel*		
TagResource	Accorde l'autorisation d'ajouter des identifications à la ressource de configuration de lecture spécifiée	Identification	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les identifications de la ressource de configuration de lecture spécifiée	Identification	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:TagKeys	
UpdateChannel	Accorde l'autorisation de mettre à jour le canal avec le nom du canal spécifié	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateLiveSource	Accorde l'autorisation de mettre à jour la source en direct avec le nom de source en direct spécifié sur l'emplacement source avec le nom de l'emplacement source spécifié	Écrire	liveSource*		
UpdateProgram	Accorde l'autorisation de supprimer le programme avec le nom de programme spécifié sur le canal avec le nom de canal spécifié	Écrire	program*		
UpdateSourceLocation	Accorde l'autorisation de mettre à jour l'emplacement source avec le nom de l'emplacement source spécifié	Écrire	sourceLocation*		
UpdateVodSource	Accorde l'autorisation de mettre à jour la source VOD avec le nom de source VOD spécifié sur l'emplacement source avec le nom de l'emplacement source spécifié	Écrire	vodSource*		

Types de ressources définis par AWS Elemental MediaTailor

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
playbackConfiguration	`arn:${Partition}:mediatailor:${Region}:${Account}:playbackConfiguration/${ResourceId}`	aws:ResourceTag/${TagKey}
prefetchSchedule	`arn:${Partition}:mediatailor:${Region}:${Account}:prefetchSchedule/${ResourceId}`	
channel	`arn:${Partition}:mediatailor:${Region}:${Account}:channel/${ChannelName}`	aws:ResourceTag/${TagKey}
program	`arn:${Partition}:mediatailor:${Region}:${Account}:program/${ChannelName}/${ProgramName}`	
sourceLocation	`arn:${Partition}:mediatailor:${Region}:${Account}:sourceLocation/${SourceLocationName}`	aws:ResourceTag/${TagKey}
vodSource	`arn:${Partition}:mediatailor:${Region}:${Account}:vodSource/${SourceLocationName}/${VodSourceName}`	aws:ResourceTag/${TagKey}
liveSource	`arn:${Partition}:mediatailor:${Region}:${Account}:liveSource/${SourceLocationName}/${LiveSourceName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Elemental MediaTailor

AWS Elemental MediaTailor définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les cas de support AWS élémentaire

AWS Elemental Support Cases (préfixe de service :`elemental-support-cases`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental Support Cases
- Types de ressources définis par AWS Elemental Support Cases
- Clés de condition pour les AWS dossiers Elemental Support

Actions définies par AWS Elemental Support Cases

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddCaseComment [autorisation uniquement]	Accorde l'autorisation d'ajouter un commentaire à un dossier de support	Écrire	case*		
CheckCasePermission [autorisation uniquement]	Accorde l'autorisation de vérifier si l'appelant dispose des autorisations nécessaires pour effectuer des opérations liées aux dossiers de support	Écrire			
CompleteMultipartUpload [autorisation uniquement]	Accorde l'autorisation de terminer le téléchargement d'un fichier en plusieurs parties vers un dossier de support	Écrire	case*		
CreateCase [autorisation uniquement]	Accorde l'autorisation de créer un dossier de support	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateS3CLIUploadCommand [autorisation uniquement]	Accorde l'autorisation de créer une commande cli pour autoriser le téléchargement d'un fichier vers un dossier de support	Écrire	case*		
CreateS3DownloadUrl [autorisation uniquement]	Autorise le téléchargement d'un fichier à partir d'un dossier de support	Écrire	case*		
GetCase [autorisation uniquement]	Accorde l'autorisation de décrire un dossier de support dans votre compte	Lecture	case*		
GetCasePermission [autorisation uniquement]	Accorde l'autorisation de vérifier si l'appelant dispose des autorisations nécessaires pour effectuer des opérations liées aux dossiers de support	Lecture			
GetCases [autorisation uniquement]	Accorde l'autorisation de répertorier les dossiers de support dans votre compte	Lecture			
GetUICache [autorisation uniquement]	Accorde l'autorisation de récupérer les données utilisateur du dossier mises en cache pour les utiliser dans la console	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForCase [autorisation uniquement]	Accorde l'autorisation de répertorier les tags sur un dossier de support	Lecture	case*		
StartMultipartUpload [autorisation uniquement]	Accorde l'autorisation de démarrer le téléchargement d'un fichier en plusieurs parties vers un dossier de support	Écrire	case*		
TagCase [autorisation uniquement]	Accorde l'autorisation d'ajouter une étiquette sur un dossier de support	Identification	case*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCase [autorisation uniquement]	Autorise le retrait d'une étiquette sur un dossier de support	Identification	case*		
				aws:TagKeys	
UpdateCase [autorisation uniquement]	Accorde l'autorisation de mettre à jour un dossier de support	Écrire	case*		
UpdateCaseStatus [autorisation uniquement]	Autorise la mise à jour du statut d'un dossier de support	Écrire	case*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMultipartUpload [autorisation uniquement]	Accorde l'autorisation de mettre à jour le téléchargement d'un fichier en plusieurs parties dans un dossier de support	Écrire	case*		

Types de ressources définis par AWS Elemental Support Cases

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
case	`arn:${Partition}:elemental-support-cases::${Account}:case/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les AWS dossiers Elemental Support

AWS Elemental Support Cases définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le contenu de support AWS élémentaire

AWS Support élémentaire (préfixe de service :`elemental-support-content`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Elemental Support Content
- Types de ressources définis par AWS Elemental Support Content
- Clés de condition pour le AWS contenu Elemental Support

Actions définies par AWS Elemental Support Content

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Query [autorisation uniquement]	Accorde l'autorisation de rechercher du contenu de support	Lecture			

Types de ressources définis par AWS Elemental Support Content

AWS Elemental Support Content ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Elemental Support Content, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le AWS contenu Elemental Support

Elemental Support Content ne dispose d'aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des instructions de politique. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon EMR on EKS (EMR Containers)

Amazon EMR on EKS (EMR Containers) (préfixe de service : `emr-containers`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EMR on EKS (EMR Containers)
- Types de ressources définis par Amazon EMR on EKS (EMR Containers)
- Clés de condition pour Amazon EMR on EKS (EMR Containers)

Actions définies par Amazon EMR on EKS (EMR Containers)

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelJobRun	Accorde l'autorisation d'annuler l'exécution d'une tâche.	Écrire	jobRun*		
CreateCertificate	Accorde l'autorisation d'appeler la CreateCertificate méthode pour accepter CertificateSigningRequest le certificat signé et le renvoyer	Écrire			
CreateJobTemplate	Accorde l'autorisation de créer un modèle de tâche	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateManagedEndpoint	Accorde l'autorisation de créer un point de terminaison géré.	Écrire	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn	
CreateSecurityConfiguration	Accorde l'autorisation de créer une configuration de sécurité.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVirtualCluster	Accorde l'autorisation de créer un cluster virtuel.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJobTemplate	Accorde l'autorisation de supprimer un modèle de tâche	Écrire	jobTemplate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteManagedEndpoint	Accorde l'autorisation de supprimer un point de terminaison géré.	Écrire	managedEndpoint*		
DeleteSecurityConfiguration	Accorde l'autorisation de supprimer une configuration de sécurité.	Écrire	securityConfiguration*		
DeleteVirtualCluster	Accorde l'autorisation de supprimer un cluster virtuel.	Écriture	virtualCluster*		
DescribeJobRun	Accorde l'autorisation de décrire l'exécution d'une tâche.	Lecture	jobRun*		
DescribeJobTemplate	Accorde l'autorisation de décrire un modèle de tâche	Lecture	jobTemplate*		
DescribeManagedEndpoint	Accorde l'autorisation de décrire un point de terminaison géré.	Lecture	managedEndpoint*		
DescribeSecurityConfiguration	Accorde l'autorisation de décrire une configuration de sécurité	Lecture	securityConfiguration*		
DescribeVirtualCluster	Accorde l'autorisation de décrire un cluster virtuel.	Lecture	virtualCluster*		
GetManagedEndpointSessionCredentials	Accorde l'autorisation de générer un jeton de session utilisé pour se connecter à un point de terminaison géré	Écrire	managedEndpoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListJobRuns	Accorde l'autorisation de créer la liste des exécutions de tâches associées à un cluster virtuel.	List	virtualCluster*		
ListJobTemplates	Accorde l'autorisation de répertorier les modèles de tâche	List			
ListManagedEndpoints	Accorde l'autorisation de créer une liste de points de terminaison gérés associés à un cluster virtuel.	List	virtualCluster*		
ListSecurityConfigurations	Accorde l'autorisation de répertorier les configurations de sécurité	List			
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée.	Liste	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListVirtualClusters	Accorde l'autorisation de répertorier les clusters virtuels.	Liste			
StartJobRun	Accorde l'autorisation de lancer l'exécution d'une tâche.	Écriture	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn emr-containers:JobTemplateArn	
TagResource	Accorde l'autorisation d'identificationr la ressource spécifiée.	Balisage	jobRun		
			jobTemplate		
			managedEndpoint		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			securityConfiguration		
			virtualCluster		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage de la ressource spécifiée.	Balisage	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		
				aws:TagKeys	

Types de ressources définis par Amazon EMR on EKS (EMR Containers)

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
virtualCluster	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}`	aws:ResourceTag/${TagKey}
jobRun	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/jobruns/${JobRunId}`	aws:ResourceTag/${TagKey}
jobTemplate	`arn:${Partition}:emr-containers:${Region}:${Account}:/jobtemplates/${JobTemplateId}`	aws:ResourceTag/${TagKey}
managedEndpoint	`arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/endpoints/${EndpointId}`	aws:ResourceTag/${TagKey}
securityConfiguration	`arn:${Partition}:emr-containers:${Region}:${Account}:/securityconfigurations/${SecurityConfigurationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon EMR on EKS (EMR Containers)

Amazon EMR on EKS (conteneurs EMR) définit les clés de condition suivantes qui peuvent être utilisées dans l' `Condition` élément d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner

les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur des balises présentes dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balises présentent dans la demande	ArrayOfString
emr-containers:ExecutionRoleArn	Filtre l'accès en fonction du rôle d'exécution arn présent dans la demande	ARN
emr-containers:JobTemplateArn	Filtre l'accès en fonction du modèle de tâche arn présent dans la demande	ARN

Actions, ressources et clés de condition pour Amazon EMR Serverless

Amazon EMR Serverless (préfixe de service : `emr-serverless`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EMR Serverless
- Types de ressources définis par Amazon EMR Serverless
- Clés de condition pour Amazon EMR Serverless

Actions définies par Amazon EMR Serverless

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AccessInteractiveEndpoints [autorisation uniquement]	Accorde l'autorisation d'exécuter des charges de travail interactives sur une application	Écrire	application*		iam:PassRole
AccessLivyEndpoints [autorisation uniquement]	Accorde l'autorisation d'exécuter des charges de travail interactives sur Livy Endpoint activé sur une application EMR sans serveur	Écrire	application*		iam:PassRole
AccessSystemProfileLogs [autorisation uniquement]	Accorde l'autorisation d'accéder aux journaux des profils du système	Écrire	jobRun*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelJobRun	Accorde l'autorisation d'annuler l'exécution d'une tâche.	Écrire	jobRun*		
CreateApplication	Accorde l'autorisation de créer une application	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	application*		
GetApplication	Accorde l'autorisation d'obtenir une application	Lecture	application*		
GetDashboardForJobRun	Accorde l'autorisation d'obtenir le tableau de board de l'exécution d'une tâche	Lecture	jobRun*		
GetJobRun	Accorde l'autorisation d'obtenir l'exécution d'une tâche	Lecture	jobRun*		
ListApplications	Accorde l'autorisation de répertorier les applications	List			
ListJobRunAttempts	Accorde l'autorisation de répertorier les tentatives d'exécution de tâches associées à une exécution de tâche	List	jobRun*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListJobRuns	Accorde l'autorisation de répertorier les exécutions de tâches associées à une application	List	application*		
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée.	Lecture	application		
			jobRun		
StartApplication	Accorde l'autorisation de démarrer une application	Écrire	application*		
StartJobRun	Accorde l'autorisation de lancer l'exécution d'une tâche.	Écrire	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopApplication	Accorde l'autorisation d'arrêter une application	Écrire	application*		
TagResource	Accorde l'autorisation d'identificationr la ressource spécifiée.	Balisage	application		
			jobRun		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage de la ressource spécifiée.	Identification	application		
			jobRun		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écrire	application*		

Types de ressources définis par Amazon EMR Serverless

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
jobRun	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}/jobruns/${JobRunId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon EMR Serverless

Amazon EMR Serverless définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS la messagerie SMS et voix de l'utilisateur final V2

AWS La version V2 de messagerie vocale et SMS destinée aux utilisateurs finaux (préfixe de service :`sms-voice`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS la messagerie, SMS et voix de l'utilisateur final (V2)
- Types de ressources définis par l'utilisateur AWS final (messagerie, SMS et voix V2)
- Clés de condition pour les messages SMS et vocaux destinés aux utilisateurs AWS finaux (V2)

Actions définies par AWS la messagerie, SMS et voix de l'utilisateur final (V2)

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateOriginationIdentity	Accorde l'autorisation d'associer un numéro de téléphone d'origine ou un ID de l'expéditeur à un groupe	Écrire	Pool*		
			PhoneNumber		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			SenderId		
AssociateProtectConfiguration	Accorde l'autorisation d'associer une configuration de protection à un ensemble de configurations	Écrire	ConfigurationSet*		
			ProtectConfiguration*		
CreateConfigurationSet	Accorde l'autorisation de créer un ensemble de configuration	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateEventDestination	Accorde l'autorisation de créer une destination d'événement dans un jeu de configuration	Écrire	ConfigurationSet*		iam:PassRole
CreateOptOutList	Accorde l'autorisation de créer une liste de désabonnement	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreatePool	Accorde l'autorisation de créer un groupe	Écrire	PhoneNumber		sms-voice:TagResource
			SenderId		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectConfiguration	Accorde l'autorisation de créer une configuration de protection	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistration	Octroie l'autorisation de créer un enregistrement.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationAssociation	Octroie l'autorisation d'associer un enregistrement à un numéro de téléphone ou à un autre enregistrement.	Écrire	Registration* PhoneNumber		
CreateRegistrationAttachment	Octroie l'autorisation de créer une pièce jointe d'enregistrement.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRegistrationVersion	Octroie l'autorisation de créer une version d'enregistrement.	Écrire	Registration*		
CreateVerifiedDestinationNumber	Octroie l'autorisation de créer un numéro de destination vérifié.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
DeleteAccountDefaultProtectConfiguration	Accorde l'autorisation de supprimer la configuration de protection par défaut du compte	Écrire			
DeleteConfigurationSet	Accorde l'autorisation de supprimer un jeu de configuration	Écrire	ConfigurationSet*		
DeleteDefaultMessageType	Accorde l'autorisation de supprimer le type de message par défaut pour un jeu de configuration	Écrire	ConfigurationSet*		
DeleteDefaultSenderId	Accorde l'autorisation de supprimer l'ID de l'expéditeur par défaut pour un jeu de configuration	Écrire	ConfigurationSet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEventDestination	Accorde l'autorisation de supprimer une destination d'événement dans un jeu de configuration	Écrire	ConfigurationSet*		
DeleteKeyword	Accorde l'autorisation de supprimer un mot clé pour un groupe ou un numéro de téléphone d'origine	Écrire	PhoneNumber		
			Pool		
DeleteMediaMessageSpendLimitOverride	Autorise la suppression d'une dérogation à la limite de dépenses mensuelles de messagerie multimédia de votre compte	Écrire			
DeleteOptOutList	Accorde l'autorisation de supprimer une liste de désabonnement	Écrire	OptOutList*		
DeleteOptedOutNumber	Accorde l'autorisation de supprimer un numéro de téléphone de destination d'une liste de désabonnement	Écrire	OptOutList*		
DeletePool	Accorde l'autorisation de supprimer un groupe d'utilisateurs	Écrire	Pool*		
DeleteProtectConfiguration	Accorde l'autorisation de supprimer une configuration de protection	Écrire	ProtectConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteProtectConfigurationRuleSetNumberOverride	Accorde l'autorisation de supprimer un numéro de téléphone en remplacement pour une configuration de protection	Écrire	ProtectConfiguration*		
DeleteRegistration	Octroie l'autorisation de supprimer un enregistrement.	Écrire	Registration*		
DeleteRegistrationAttachment	Octroie l'autorisation de supprimer une pièce jointe d'enregistrement.	Écrire	RegistrationAttachment*		
DeleteRegistrationFieldValue	Octroie l'autorisation de supprimer une valeur facultative de champ d'enregistrement.	Écrire	Registration*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource.	Gestion des autorisations	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
DeleteTextMessageSpendLimitOverride	Accorde l'autorisation de supprimer une dérogation à la limite de dépenses mensuelles de messagerie SMS de votre compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteVerifiedDestinationNumber	Octroie l'autorisation de supprimer un numéro de destination vérifié.	Écrire	VerifiedDestinationNumber*		
DeleteVoiceMessageSpendLimitOverride	Accorde l'autorisation de supprimer une dérogation à la limite de dépenses mensuelles de messagerie vocale de votre compte	Écrire			
DescribeAccountAttributes	Accorde l'autorisation de décrire les attributs de votre compte	Lecture			
DescribeAccountLimits	Accorde l'autorisation de décrire les Service Quotas pour votre compte	Lecture			
DescribeConfigurationSets	Accorde l'autorisation de décrire les jeux de configurations dans votre compte	Lecture	ConfigurationSet		
DescribeKeywords	Accorde l'autorisation de décrire un mot clé pour un groupe ou un numéro de téléphone d'origine	Lecture	PhoneNumber		
			Pool		
DescribeOptOutLists	Accorde l'autorisation de décrire les listes de désabonnement dans votre compte	Lecture	OptOutList		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeOptedOutNumbers	Accorde l'autorisation de décrire les numéros de téléphone de destination dans une liste de désabonnement	Lecture	OptOutList*		
DescribePhoneNumbers	Accorde l'autorisation de décrire les numéros de téléphone d'origine dans votre compte	Lecture	PhoneNumber		
DescribePools	Accorde l'autorisation de décrire les groupes dans votre compte	Lecture	Pool		
DescribeProtectConfigurations	Accorde l'autorisation de décrire les configurations de protection de votre compte	Lecture	ProtectConfiguration		
DescribeRegistrationAttachments	Octroie l'autorisation de décrire les pièces jointes d'enregistrement de votre compte.	Lecture	RegistrationAttachment		
DescribeRegistrationFieldDefinitions	Octroie l'autorisation de décrire les définitions de champ d'un type d'enregistrement donné.	Lecture			
DescribeRegistrationFieldValues	Octroie l'autorisation de décrire les valeurs de champ d'un enregistrement donné.	Lecture	Registration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRegistrationSectionDefinitions	Octroie l'autorisation de décrire les définitions de section d'un type d'enregistrement donné.	Lecture			
DescribeRegistrationTypeDefinitions	Octroie l'autorisation de décrire les types d'enregistrement pris en charge par le service.	Lecture			
DescribeRegistrationVersions	Octroie l'autorisation de décrire les versions d'un enregistrement donné.	Lecture	Registration*		
DescribeRegistrations	Octroie l'autorisation de décrire les enregistrements de votre compte.	Lecture	Registration		
DescribeSenderIds	Permet de décrire l'expéditeur IDs de votre compte	Lecture	SenderId		
DescribeSpendLimits	Accorde l'autorisation de décrire les limites de dépenses mensuelles pour votre compte	Lecture			
DescribeVerifiedDestinationNumbers	Octroie l'autorisation de décrire les numéros de destination vérifiés de votre compte.	Lecture	VerifiedDestinationNumber		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateOriginationIdentity	Accorde l'autorisation de dissocier un numéro de téléphone d'origine ou un ID de l'expéditeur d'un groupe	Écrire	Pool*		
			PhoneNumber		
			SenderId		
DisassociateProtectConfiguration	Accorde l'autorisation de dissocier une configuration de protection d'un ensemble de configurations	Écrire	ConfigurationSet*		
			ProtectConfiguration*		
DiscardRegistrationVersion	Octroie l'autorisation d'ignorer la dernière version d'un enregistrement donné.	Écrire	Registration*		
GetProtectConfigurationCountryRuleSet	Accorde l'autorisation d'obtenir la règle de pays définie pour une configuration de protection	Lecture	ProtectConfiguration*		
GetResourcePolicy	Accorde l'autorisation d'obtenir une stratégie de ressource	Lecture	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPoolOriginationIdentities	Accorde l'autorisation de répertorier tous les numéros de téléphone d'origine et tous les expéditeurs IDs associés à un pool	Lecture	Pool*		
ListProtectConfigurationRuleSetNumberOverrides	Accorde l'autorisation de répertorier toutes les remplacements de numéros de téléphone pour une configuration de protection	Lecture	ProtectConfiguration*		
ListRegistrationAssociations	Octroie l'autorisation de répertorier toutes les ressources associées à un enregistrement.	Lecture	Registration*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Registration		
			RegistrationAttachment		
			SenderId		
			VerifiedDestinationNumber		
PutKeyword	Accorde l'autorisation de créer ou de mettre à jour un mot clé pour un groupe ou un numéro de téléphone d'origine	Écrire	PhoneNumber		
			Pool		
PutMessageFeedback	Accorde l'autorisation de publier des commentaires pour un message texte, vocal ou multimédia	Écrire	Message*		
PutOptedOutNumber	Accorde l'autorisation de placer un numéro de téléphone de destination dans une liste de désabonnement	Écrire	OptOutList*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutProtectConfigurationRuleSetNumberOverride	Accorde l'autorisation de remplacer un numéro de téléphone pour une configuration de protection	Écrire	ProtectConfiguration*		
PutRegistrationFieldValue	Octroie l'autorisation de saisir une valeur de champ d'enregistrement.	Écrire	Registration*		
PutResourcePolicy	Octroie l'autorisation de saisir une stratégie de ressources.	Gestion des autorisations	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
ReleasePhoneNumber	Accorde l'autorisation de libérer un numéro de téléphone d'origine	Écrire	PhoneNumber*		
ReleaseSenderId	Octroie l'autorisation de diffuser un ID d'expéditeur.	Écrire	SenderId*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RequestPhoneNumber	Accorde l'autorisation de demander un numéro de téléphone d'origine	Écrire	Pool		sms-voice:AssociateOriginationIdentity sms-voice:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
RequestSenderId	Octroie l'autorisation de demander un ID d'expéditeur non enregistré.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendDestinationNumberVerificationCode	Octroie l'autorisation d'envoyer un message textuel ou vocal contenant un code de vérification à un numéro de téléphone de destination.	Écrire	PhoneNumber		sms-voice:SendTextMessage sms-voice:SendVoiceMessage
			Pool		
			SenderId		
SendMediaMessage	Accorde l'autorisation d'envoyer un message multimédia à un numéro de téléphone de destination	Écrire	PhoneNumber		
			Pool		
SendTextMessage	Accorde l'autorisation d'envoyer un message SMS à un numéro de téléphone de destination	Écrire	PhoneNumber		
			Pool		
			SenderId		
SendVoiceMessage	Accorde l'autorisation d'envoyer un message vocal à un numéro de téléphone de destination	Écrire	PhoneNumber		
			Pool		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetAccountDefaultProtectConfiguration	Accorde l'autorisation de définir une configuration de protection par défaut pour le compte	Écrire	ProtectConfiguration*		
SetDefaultMessageFeedbackEnabled	Accorde l'autorisation de définir le message de feedback par défaut pour un ensemble de configurations	Écrire	ConfigurationSet*		
SetDefaultMessageType	Accorde l'autorisation de définir le type de message par défaut pour un jeu de configuration	Écrire	ConfigurationSet*		
SetDefaultSenderId	Accorde l'autorisation de définir l'ID de l'expéditeur par défaut pour un jeu de configuration	Écrire	ConfigurationSet*		
SetMediaMessageSpendLimitOverride	Accorde l'autorisation de définir une dérogation à la limite de dépenses mensuelles de messagerie multimédia de votre compte	Écrire			
SetTextMessageSpendLimitOverride	Accorde l'autorisation de définir une dérogation à la limite de dépenses mensuelles de messagerie SMS de votre compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetVoiceMessageSpendLimitOverride	Accorde l'autorisation de définir une dérogation à la limite de dépenses mensuelles de messagerie vocale de votre compte	Écrire			
SubmitRegistrationVersion	Octroie l'autorisation de soumettre la dernière version d'un enregistrement donné.	Écrire	Registration*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			VerifiedDestinationNumber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			SenderId		
			VerifiedDestinationNumber		
				aws:TagKeys	
UpdateEventDestination	Accorde l'autorisation de mettre à jour la destination de l'événement d'un jeu de configurations	Écrire	ConfigurationSet*		iam:PassRole
UpdatePhoneNumber	Accorde l'autorisation de mettre à jour la configuration d'un numéro de téléphone d'origine	Écrire	PhoneNumber*		iam:PassRole
UpdatePool	Accorde l'autorisation de mettre à jour une configuration de groupe	Écrire	Pool*		iam:PassRole
UpdateProtectConfiguration	Accorde l'autorisation de mettre à jour une configuration de protection	Écrire	ProtectConfiguration*		
UpdateProtectConfigurationCountryRuleSet	Accorde l'autorisation de mettre à jour un ensemble de règles de pays pour une configuration de protection	Écrire	ProtectConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSenderId	Octroie l'autorisation de mettre à jour une configuration d'ID d'expéditeur.	Écrire	SenderId*		
VerifyDestinationNumber	Octroie l'autorisation de vérifier un numéro de téléphone de destination.	Écrire	VerifiedDestinationNumber*		

Types de ressources définis par l'utilisateur AWS final (messagerie, SMS et voix V2)

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
ConfigurationSet	`arn:${Partition}:sms-voice:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
OptOutList	`arn:${Partition}:sms-voice:${Region}:${Account}:opt-out-list/${OptOutListName}`	aws:ResourceTag/${TagKey}
PhoneNumber	`arn:${Partition}:sms-voice:${Region}:${Account}:phone-number/${PhoneNumberId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Pool	arn:${Partition}:sms-voice:${Region}:${Account}:pool/${PoolId}	aws:ResourceTag/${TagKey}
ProtectConfiguration	arn:${Partition}:sms-voice:${Region}:${Account}:protect-configuration/${ProtectConfigurationId}	aws:ResourceTag/${TagKey}
SenderId	arn:${Partition}:sms-voice:${Region}:${Account}:sender-id/${SenderId}/${IsoCountryCode}	aws:ResourceTag/${TagKey}
Registration	arn:${Partition}:sms-voice:${Region}:${Account}:registration/${RegistrationId}	aws:ResourceTag/${TagKey}
RegistrationAttachment	arn:${Partition}:sms-voice:${Region}:${Account}:registration-attachment/${RegistrationAttachmentId}	aws:ResourceTag/${TagKey}
VerifiedDestinationNumber	arn:${Partition}:sms-voice:${Region}:${Account}:verified-destination-number/${VerifiedDestinationNumberId}	aws:ResourceTag/${TagKey}
Message	arn:${Partition}:sms-voice:${Region}:${Account}:message/${MessageId}	

Clés de condition pour les messages SMS et vocaux destinés aux utilisateurs AWS finaux (V2)

AWS La version V2 des messages SMS et voix destinés aux utilisateurs finaux définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS la messagerie sociale destinée aux utilisateurs finaux

AWS End User Messaging Social (préfixe de service :`social-messaging`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'utilisateur AWS final Messaging Social
- Types de ressources définis par AWS End User Messaging Social
- Clés de condition pour AWS la messagerie sociale destinée aux utilisateurs finaux

Actions définies par l'utilisateur AWS final Messaging Social

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateWhatsAppBusinessAccount	Accorde l'autorisation d'associer un compte WhatsApp professionnel à votre Compte AWS	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateWhatsAppMessageTemplate	Accorde l'autorisation de créer un modèle de WhatsApp message	Écrire	waba*		
CreateWhatsAppMessageTemplateFromLibrary	Accorde l'autorisation de créer un modèle de WhatsApp message à partir de la bibliothèque de modèles de Meta	Écrire	waba*		
CreateWhatsAppMessageTemplateMedia	Accorde l'autorisation de créer des médias pour les modèles de WhatsApp messages	Écrire	waba*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteWhatsAppMessageMedia	Accorde l'autorisation de supprimer un objet multimédia de WhatsApp	Écrire	phone-number-id*		
DeleteWhatsAppMessageTemplate	Accorde l'autorisation de supprimer un modèle de WhatsApp message	Écrire	waba*		
DisassociateWhatsAppBusinessAccount	Accorde l'autorisation de dissocier un compte WhatsApp professionnel de votre Compte AWS	Écrire	waba*		
GetLinkedWhatsAppBusinessAccount	Autorise l'accès aux détails d'un compte WhatsApp professionnel	Lecture	waba*		
GetLinkedWhatsAppBusinessAccountPhoneNumber	Accorde l'autorisation de consulter les détails d'un numéro de téléphone	Lecture	phone-number-id*		
GetWhatsAppMessageMedia	Accorde l'autorisation d'obtenir un objet multimédia auprès de WhatsApp	Écrire	phone-number-id*		
GetWhatsAppMessageTemplate	Accorde l'autorisation d'obtenir les détails d'un modèle de WhatsApp message	Lecture	waba*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLinkedWhatsAppBusinessAccounts	Autorise l'accès à tous vos comptes WhatsApp professionnels	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	phone-number-id		
			waba		
ListWhatsAppMessageTemplates	Accorde l'autorisation de répertorier les modèles de WhatsApp messages	List	waba*		
ListWhatsAppTemplateLibrary	Accorde l'autorisation de répertorier les modèles disponibles dans la bibliothèque de modèles de Meta	List	waba*		
PostWhatsAppMessageMedia	Accorde l'autorisation de télécharger un objet multimédia sur WhatsApp	Écrire	phone-number-id*		
PutWhatsAppBusinessAccountEventDestinations	Autorise la mise à jour de la destination WhatsApp d'un événement Business Accounts	Écrire	waba*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendWhatsAppMessage	Accorde l'autorisation d'envoyer un message via WhatsApp	Écrire	phone-number-id*		
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource	Balisage	phone-number-id		
			waba		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	phone-number-id		
			waba		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateWhatsAppMessageTemplate	Accorde l'autorisation de mettre à jour un modèle de WhatsApp message	Écrire	waba*		

Types de ressources définis par AWS End User Messaging Social

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
phone-number-id	`arn:${Partition}:social-messaging:${Region}:${Account}:phone-number-id/${OriginationPhoneNumberId}`	aws:ResourceTag/${TagKey}
waba	`arn:${Partition}:social-messaging:${Region}:${Account}:waba/${WabaId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS la messagerie sociale destinée aux utilisateurs finaux

AWS End User Messaging Social définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour la résolution AWS d'entités

AWS Entity Resolution (préfixe de service :`entityresolution`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Entity Resolution
- Types de ressources définis par AWS Entity Resolution
- Clés de condition pour la résolution AWS d'entités

Actions définies par AWS Entity Resolution

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddPolicyStatement	Accorde l'autorisation de donner à un AWS service ou à un autre compte l'autorisation d'utiliser les ressources d'une AWS Entity Resolution	Gestion des autorisations			
BatchDeleteUniqueId	Autorise la suppression par lots de l'identifiant unique	Écrire	MatchingWorkflow*		
CreateIdMappingWorkflow	Accorde l'autorisation de créer un flux de travail idmapping.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIdNamespace	Accorde l'autorisation de créer un IdNamespace	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMatchingWorkflow	Octroie l'autorisation de créer un flux de travail correspondant.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSchemaMapping	Octroie l'autorisation de créer un mappage de schéma.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdMappingWorkflow	Accorde l'autorisation de supprimer un flux de travail idmapping.	Écrire	IdMappingWorkflow*		
DeleteIdNamespace	Accorde l'autorisation de supprimer un IdNamespace	Écrire	IdNamespace*		
DeleteMatchingWorkflow	Octroie l'autorisation de supprimer un flux de travail correspondant.	Écrire	MatchingWorkflow*		
DeletePolicyStatement	Accorde l'autorisation de supprimer l'autorisation accordée à un AWS service ou à un autre compte, l'autorisation d'utiliser les ressources d'une AWS entité de résolution	Gestion des autorisations			
DeleteSchemaMapping	Octroie l'autorisation de supprimer un mappage de schéma.	Écrire	SchemaMapping*		
GenerateMatchId	Accorde l'autorisation de générer un identifiant de correspondance	Écrire	MatchingWorkflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetIdMappingJob	Accorde l'autorisation d'obtenir une tâche idmapping.	Lecture	IdMappingWorkflow*		
GetIdMappingWorkflow	Accorde l'autorisation d'obtenir un flux de travail idmapping.	Lecture	IdMappingWorkflow*		
GetIdNamespace	Donne l'autorisation d'obtenir un IdNamespace	Lecture	IdNamespace*		
GetMatchId	Octroie l'autorisation d'obtenir un ID correspondant.	Lecture	MatchingWorkflow*		
GetMatchingJob	Octroie l'autorisation d'obtenir une tâche correspondante.	Lecture	MatchingWorkflow*		
GetMatchingWorkflow	Octroie l'autorisation d'obtenir un flux de travail correspondant.	Lecture	MatchingWorkflow*		
GetPolicy	Accorde l'autorisation d'obtenir une politique de ressources pour une AWS entité (ressources de résolution)	Lecture			
GetProviderService	Accorde l'autorisation d'obtenir le service de fournisseur.	Lecture	ProviderService*		
GetSchemaMapping	Octroie l'autorisation d'obtenir un mappage de schéma.	Lecture	SchemaMapping*		
ListIdMappingJobs	Accorde l'autorisation de répertorier les tâches idmapping.	List	IdMappingWorkflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIdMappingWorkflows	Accorde l'autorisation de répertorier les flux de travail idmapping.	List			
ListIdNamespaces	Accorde l'autorisation de mettre en vente IdNamespaces	List			
ListMatchingJobs	Octroie l'autorisation de répertorier les tâches correspondantes.	List	MatchingWorkflow*		
ListMatchingWorkflows	Octroie l'autorisation de répertorier les flux de travail correspondants.	List			
ListProviderServices	Accorde l'autorisation de répertorier les services de fournisseurs.	List			
ListSchemaMappings	Octroie l'autorisation de répertorier les mappages de schémas.	List			
ListTagsForResource	Octroie l'autorisation de répertorier les balises d'une ressource.	Lecture			
PutPolicy	Autorise la mise en place d'une politique de ressources pour une AWS entité (ressources de résolution)	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartIdMappingJob	Accorde l'autorisation de démarrer une tâche idmapping.	Écrire	IdMappingWorkflow*		
StartMatchingJob	Octroie l'autorisation de lancer une tâche correspondante.	Écrire	MatchingWorkflow*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Identification	IdMappingWorkflow		
			IdNamespace		
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	IdMappingWorkflow		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			IdNamespace		
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:TagKeys	
UpdateIdMappingWorkflow	Accorde l'autorisation de mettre à jour un flux de travail idmapping.	Écrire	IdMappingWorkflow*		
UpdateIdNamespace	Accorde l'autorisation de mettre à jour un IdNamespace	Écrire	IdNamespace*		
UpdateMatchingWorkflow	Octroie l'autorisation de mettre à jour un flux de travail correspondant.	Écrire	MatchingWorkflow*		
UpdateSchemaMapping	Accorde l'autorisation de mettre à jour un mappage de schéma.	Écrire	SchemaMapping*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UseIdNamespace	Accorde l'autorisation d'autoriser un AWS service ou un autre compte à utiliser IdNamespace dans un flux de travail	Gestion des autorisations			
UseWorkflow	Accorde l'autorisation d'autoriser un AWS service ou un autre compte à utiliser le flux de travail dans un IdNamespace	Gestion des autorisations			

Types de ressources définis par AWS Entity Resolution

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
MatchingWorkflow	`arn:${Partition}:entityresolution:${Region}:${Account}:matchingworkflow/${WorkflowName}`	aws:ResourceTag/${TagKey}
SchemaMapping	`arn:${Partition}:entityresolution:${Region}:${Account}:schemamapping/${SchemaName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
IdMappingWorkflow	arn:${Partition}:entityresolution:${Region}:${Account}:idmappingworkflow/${WorkflowName}	aws:ResourceTag/${TagKey}
ProviderService	arn:${Partition}:entityresolution:${Region}:${Account}:providerservice/${ProviderName}/${ProviderServiceName}	aws:ResourceTag/${TagKey}
IdNamespace	arn:${Partition}:entityresolution:${Region}:${Account}:idnamespace/${IdNamespaceName}	aws:ResourceTag/${TagKey}

Clés de condition pour la résolution AWS d'entités

AWS Entity Resolution définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'une clé qui est présente dans la demande envoyée par l'utilisateur au service Entity Resolution.	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction d'une paire de clé et de valeur de balise	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction de la liste de tous les noms de clé de balise présents dans la demande envoyée par l'utilisateur au service Entity Resolution.	ArrayOfString

Actions, ressources et clés de condition pour Amazon EventBridge

Amazon EventBridge (préfixe de service :`events`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EventBridge
- Types de ressources définis par Amazon EventBridge
- Clés de condition pour Amazon EventBridge

Actions définies par Amazon EventBridge

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateEventSource	Accorde l'autorisation d'activer les sources d'événements d'un partenaire.	Écrire	event-source*		
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux vendus pour EventBridge	Écrire	event-bus*		
CancelReplay	Accorde l'autorisation d'annuler une relecture.	Écriture	replay*		
CreateApiDestination	Accorde l'autorisation de créer une destination d'API	Écriture	api-destination*		
			connection*		
CreateArchive	Accorde l'autorisation de créer une archive.	Écriture	archive*		
			event-bus*		
			alias		
			key		
CreateConnection	Accorde l'autorisation de créer une connexion	Écrire	connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEndpoint	accorde l'autorisation de créer un point de terminaison	Écrire	endpoint*		
				events:EventBusArn	
CreateEventBus	Accorde l'autorisation de créer des bus d'événements.	Écriture	event-bus*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerEventSource	Accorde l'autorisation de créer les sources d'événements d'un partenaire.	Écriture	event-source*		
DeactivateEventSource	Accorde l'autorisation de désactiver des sources d'événements.	Écriture	event-source*		
DeauthorizeConnection	Accorde l'autorisation de retirer une autorisation de connexion, en supprimant ses secrets d'autorisation stockés	Écriture	connection*		
DeleteApiDestination	Accorde l'autorisation de supprimer une destination d'API	Écriture	api-destination*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteArchive	Accorde l'autorisation de supprimer une archive.	Écriture	archive*		
DeleteConnection	Accorde l'autorisation de supprimer une connexion.	Écrire	connection*		
DeleteEndpoint	Accorde l'autorisation de supprimer un point de terminaison	Écrire	endpoint*		
DeleteEventBus	Accorde l'autorisation de supprimer des bus d'événements.	Écriture	event-bus*		
DeletePartnerEventSource	Accorde l'autorisation de supprimer les sources d'événements d'un partenaire.	Écriture	event-source*		
DeleteRule	Accorde l'autorisation de supprimer des règles.	Écriture	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeApiDestination	Accorde l'autorisation de récupérer des informations sur une destination d'API	Lecture	api-destination* connection*		
DescribeArchive	Accorde l'autorisation de récupérer des informations sur une archive.	Lecture	archive*		
DescribeConnection	Accorde l'autorisation de récupérer des informations sur une connexion	Lecture	connection*		
DescribeEndpoint	Accorde l'autorisation de récupérer des détails sur un point de terminaison	Lecture	endpoint*		
DescribeEventBus	Accorde l'autorisation de récupérer des informations sur les bus d'événements.	Lecture	event-bus		
DescribeEventSource	Accorde l'autorisation de récupérer des informations sur les sources d'événements.	Lecture	event-source*		
DescribePartnerEventSource	Accorde l'autorisation de récupérer des informations sur les sources d'événements d'un partenaire.	Lecture	event-source*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReplay	Accorde l'autorisation de récupérer des informations d'une relecture.	Lecture	replay*		
DescribeRule	Accorde l'autorisation de récupérer des informations sur les règles.	Lecture	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
DisableRule	Accorde l'autorisation de désactiver des règles.	Écrire	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableRule	Accorde l'autorisation d'activer des règles.	Écrire	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
InvokeApiDestination [autorisation uniquement]	Accorde l'autorisation d'appeler une destination d'API	Écriture	api-destination*		
ListApiDestinations	Accorde l'autorisation de récupérer une liste de destinations d'API	Liste			
ListArchives	Accorde l'autorisation de récupérer une liste d'archives.	Liste			
ListConnections	Accorde l'autorisation de récupérer une liste de connexions.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEndpoints	Accorde l'autorisation de récupérer une liste de points de terminaison	List			
ListEventBuses	Accorde l'autorisation de récupérer une liste des bus d'événements dans votre compte	List			
ListEventSources	Accorde l'autorisation de récupérer une liste de sources d'événements partagées avec ce compte.	List			
ListPartnerEventSourceAccounts	Accorde l'autorisation de récupérer une liste de sources Compte AWS IDs associées à un événement	List	event-source*		
ListPartnerEventSources	Accorde l'autorisation de récupérer une liste de sources d'événements d'un partenaire.	Liste			
ListReplays	Accorde l'autorisation de récupérer une liste de relectures.	Liste			
ListRuleNamesByTarget	Accorde l'autorisation de récupérer une liste des noms des règles associées à une cible.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRules	Accorde l'autorisation de récupérer une liste des EventBridge règles Amazon dans le compte	List			
ListTagsForResource	Accorde l'autorisation de récupérer une liste de balises associées à une EventBridge ressource Amazon	List	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
ListTargetsByRule	Accorde l'autorisation de récupérer une liste de cibles définies pour une règle.	List	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				events:creatorAccount	
PutEvents	Accorde l'autorisation d'envoyer des événements personnalisés à Amazon EventBridge	Écrire	event-bus*		
				events:detail-type events:source events:eventBusInvocation	
PutPartnerEvents	Accorde l'autorisation d'envoyer des événements personnalisés à Amazon EventBridge	Écrire			
PutPermission	Accorde l'autorisation d'utiliser l' PutPermission action pour autoriser une autre personne Compte AWS à placer des événements dans votre bus d'événements par défaut	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutRule	Accorde l'autorisation de créer ou de mettre à jour des règles.	Écrire	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutTargets	Accorde l'autorisation d'ajouter des cibles à une règle.	Écrire	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	Accorde l'autorisation de révoquer l'autorisation d'une autre personne d'Compte AWS ajouter des événements à votre bus d'événements par défaut	Gestion des autorisations			
RemoveTargets	Accorde l'autorisation de supprimer des cibles d'une règle.	Écrire	rule-on-custom-event-bus		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials [autorisation uniquement]	Octroie l'autorisation de récupérer des informations d'identification à partir d'une connexion.	Écrire	connection*		
StartReplay	Accorde l'autorisation de lancer une relecture d'une archive.	Écrire	archive*		
			event-bus*		
			replay*		
TagResource	Accorde l'autorisation d'ajouter un tag à une EventBridge ressource Amazon	Identification	event-bus		
			rule-on-custom-event-bus		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			rule-on-default-event-bus		
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	Accorde l'autorisation de tester si un modèle d'événement correspond à l'événement fourni.	Lecture			
UntagResource	Accorde l'autorisation de supprimer un tag d'une EventBridge ressource Amazon	Identification	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys events:creatorAccount	
UpdateApiDestination	Accorde l'autorisation de mettre à jour une destination d'API	Écriture	api-destination*		
UpdateArchive	Accorde l'autorisation de mettre à jour une archive.	Écriture	archive*		
			alias		
			key		
UpdateConnection	Accorde l'autorisation de mettre à jour une connexion.	Écrire	connection*		
UpdateEndpoint	Accorde l'autorisation de mettre à jour un point de terminaison	Écrire	endpoint*		
				events:EventBusArn	
UpdateEventBus	Accorde l'autorisation de mettre à jour les bus des événements	Écrire	event-bus*		

Types de ressources définis par Amazon EventBridge

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
event-source	`arn:${Partition}:events:${Region}::event-source/${EventSourceName}`	
event-bus	`arn:${Partition}:events:${Region}:${Account}:event-bus/${EventBusName}`	aws:ResourceTag/${TagKey}
rule-on-default-event-bus	`arn:${Partition}:events:${Region}:${Account}:rule/${RuleName}`	aws:ResourceTag/${TagKey}
rule-on-custom-event-bus	`arn:${Partition}:events:${Region}:${Account}:rule/${EventBusName}/${RuleName}`	aws:ResourceTag/${TagKey}
archive	`arn:${Partition}:events:${Region}:${Account}:archive/${ArchiveName}`	
replay	`arn:${Partition}:events:${Region}:${Account}:replay/${ReplayName}`	
connection	`arn:${Partition}:events:${Region}:${Account}:connection/${ConnectionName}`	
api-destination	`arn:${Partition}:events:${Region}:${Account}:api-destination/${ApiDestinationName}`	
endpoint	`arn:${Partition}:events:${Region}:${Account}:endpoint/${EndpointName}`	

Types de ressources	ARN	Clés de condition
create-snapshot	arn:${Partition}:events:${Region}:${Account}:target/create-snapshot	
reboot-instance	arn:${Partition}:events:${Region}:${Account}:target/reboot-instance	
stop-instance	arn:${Partition}:events:${Region}:${Account}:target/stop-instance	
terminate-instance	arn:${Partition}:events:${Region}:${Account}:target/terminate-instance	
alias	arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}	
key	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Clés de condition pour Amazon EventBridge

Amazon EventBridge définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès au bus d'événements et aux actions de règle en fonction de l'ensemble de valeurs autorisé pour chacune des balises	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès au bus d'événements et aux actions de règle en fonction de la valeur-balise associée à la ressource	String
aws:TagKeys	Filtre l'accès au bus d'événements et aux actions de règle en fonction des balises dans la demande	ArrayOfString
events:EventBusArn	Filtre l'accès par l'ARN des bus d'événements qui peuvent être associés à un point de terminaison CreateEndpoint et à UpdateEndpoint des actions	ArrayOfARN
events:ManagedBy	Filtre l'accès par AWS services. Si une règle est créée par un AWS service en votre nom, la valeur est le nom principal du service qui a créé la règle	String
events:TargetArn	Filtre l'accès par l'ARN d'une cible qui peut être assigné à une règle aux PutTargets actions. TargetArn n'inclut pas DeadLetterConfigArn	ArrayOfARN
events:creatorAccount	Filtre l'accès aux actions de règle en fonction du compte à partir duquel la règle a été créée	String
events:detail-type	Filtre l'accès en fonction de la chaîne littérale du type de détail de l'événement et des actions PutEvents PutRule	ArrayOfString
events:detail.eventTypeCode	Filtre l'accès par chaîne littérale pour les détails. eventTypeCode champ de l'événement aux PutRule actions	String
events:detail.service	Filtre l'accès par la chaîne littérale du champ detail.service de l'événement aux actions PutRule	String
events:detail.userIdentity.principalId	Filtre l'accès par la chaîne littérale du champ detail.useridentity.principalid de l'événement aux actions PutRule	String

Clés de condition	Description	Type
events:eventBusInvocation	Filtre l'accès selon que l'événement a été généré via une API ou un appel de bus entre comptes à des actions PutEvents	String
events:source	Filtre l'accès en AWS fonction du service ou de la source d'événement AWS partenaire qui a généré l'événement PutEvents et PutRule les actions. Correspond à la chaîne littérale du champ source de l'événement	ArrayOfString

Actions, ressources et clés de condition pour Amazon EventBridge Pipes

Amazon EventBridge Pipes (préfixe de service :`pipes`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EventBridge Pipes
- Types de ressources définis par Amazon EventBridge Pipes
- Clés de condition pour Amazon EventBridge Pipes

Actions définies par Amazon EventBridge Pipes

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePipe	Accorde l'autorisation de créer un canal	Écrire	pipe*		iam:PassRole
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeletePipe	Accorde l'autorisation de supprimer un canal	Écrire	pipe*		
				aws:ResourceTag/${TagKey}	
DescribePipe	Accorde l'autorisation de décrire un canal	Lecture	pipe*		
				aws:ResourceTag/${TagKey}	
ListPipes	Accorde l'autorisation de répertorier tous les canaux dans votre compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	pipe*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
StartPipe	Accorde l'autorisation de démarrer un canal	Écrire	pipe*		
				aws:ResourceTag/${TagKey}	
StopPipe	Accorde l'autorisation d'arrêter un canal	Écrire	pipe*		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	pipe*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	pipe*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePipe	Accorde l'autorisation de mettre à jour un canal	Écrire	pipe*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon EventBridge Pipes

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
pipe	`arn:${Partition}:pipes:${Region}:${Account}:pipe/${Name}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon EventBridge Pipes

Amazon EventBridge Pipes définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des étiquettes	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon EventBridge Scheduler

Amazon EventBridge Scheduler (préfixe de service :`scheduler`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EventBridge Scheduler

- Types de ressources définis par Amazon EventBridge Scheduler
- Clés de condition pour Amazon EventBridge Scheduler

Actions définies par Amazon EventBridge Scheduler

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSchedule	Accorde l'autorisation de créer un calendrier Amazon EventBridge Scheduler	Écrire	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	
CreateScheduleGroup	Accorde l'autorisation de créer un groupe de planification Amazon EventBridge Scheduler	Écrire	schedule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSchedule	Autorise la suppression d'un calendrier Amazon EventBridge Scheduler	Écrire	schedule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteScheduleGroup	Autorise la suppression d'un groupe de planning Amazon EventBridge Scheduler	Écrire	schedule-group*		scheduler:DeleteSchedule
				aws:ResourceTag/${TagKey}	
GetSchedule	Autorise l'accès aux informations relatives à un calendrier Amazon EventBridge Scheduler	Lecture	schedule*		
				aws:ResourceTag/${TagKey}	
GetScheduleGroup	Autorise l'accès aux informations relatives à un groupe de planification Amazon EventBridge Scheduler	Lecture	schedule-group*		
				aws:ResourceTag/${TagKey}	
ListScheduleGroups	Accorde l'autorisation de répertorier les groupes de planification Amazon EventBridge Scheduler dans votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSchedules	Accorde l'autorisation de répertorier les plannings Amazon EventBridge Scheduler dans votre compte	List			
ListTagsForResource	Accorde l'autorisation de créer une balise de liste pour une ressource Amazon EventBridge Scheduler	Lecture	schedule-group		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource Amazon EventBridge Scheduler	Identification	schedule-group*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource Amazon EventBridge Scheduler	Identification	schedule-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateSchedule	Accorde l'autorisation de modifier un calendrier Amazon EventBridge Scheduler	Écrire	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon EventBridge Scheduler

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
schedule-group	`arn:${Partition}:scheduler:${Region}:${Account}:schedule-group/${GroupName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
schedule	`arn:${Partition}:scheduler:${Region}:${Account}:schedule/${GroupName}/${ScheduleName}`	

Clés de condition pour Amazon EventBridge Scheduler

Amazon EventBridge Scheduler définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString

Actions, ressources et clés de condition pour Amazon EventBridge Schemas

Amazon EventBridge Schemas (préfixe de service :`schemas`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon EventBridge Schemas
- Types de ressources définis par Amazon EventBridge Schemas
- Clés de condition pour Amazon EventBridge Schemas

Actions définies par Amazon EventBridge Schemas

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDiscoverer	Accorde l'autorisation de créer un détecteur de schéma d'événement. Une fois créés, vos événements sont automatiquement mappés dans les documents de schéma correspondants	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegistry	Accorde l'autorisation de créer un registre de schémas dans votre compte	Écrire	registry*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Accorde l'autorisation de créer un schéma dans votre compte	Écrire	schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDiscoverer	Accorde l'autorisation de supprimer le détecteur dans votre compte	Écrire	discoverer*		
DeleteRegistry	Accorde l'autorisation de supprimer un registre existant dans votre compte	Écrire	registry*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique basée sur les ressources attachée à un registre donné	Écrire	registry*		
DeleteSchema	Accorde l'autorisation de supprimer un schéma existant dans votre compte	Écrire	schema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSchemaVersion	Accorde l'autorisation de supprimer une version spécifique de schéma dans votre compte	Écrire	schema*		
DescribeCodeBinding	Accorde l'autorisation de récupérer les métadonnées du code généré pour un schéma spécifique dans votre compte	Lecture	schema*		
DescribeDiscoverer	Accorde l'autorisation de récupérer les métadonnées du détecteur dans votre compte	Lecture	discoverer*		
DescribeRegistry	Accorde l'autorisation de décrire les métadonnées d'un registre existant dans votre compte	Lecture	registry*		
DescribeSchema	Accorde l'autorisation de récupérer un schéma existant dans votre compte	Lecture	schema*		
ExportSchema	Autorise l'exportation du AWS registre ou des schémas découverts au format OpenAPI 3 vers le format JSONSchema	Lecture	registry* schema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCodeBindingSource	Accorde l'autorisation de récupérer les métadonnées du code généré pour un schéma spécifique dans votre compte	Lecture	schema*		
GetDiscoveredSchema	Accorde l'autorisation de récupérer le schéma de la liste d'exemples d'événements fournie	Lecture			
GetResourcePolicy	Accorde l'autorisation de récupérer la politique basée sur les ressources attachée à un registre donné	Lecture	registry*		
ListDiscoverers	Accorde l'autorisation de répertorier tous les détecteurs dans votre compte	List	discoverer*		
ListRegistries	Accorde l'autorisation de répertorier tous les registres dans votre compte	List	registry*		
ListSchemaVersions	Accorde l'autorisation de répertorier toutes les versions d'un thème	List	schema*		
ListSchemas	Accorde l'autorisation de répertorier tous les schémas	List	schema*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture	discoverer		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			registry		
			schema		
PutCodeBinding	Accorde l'autorisation de générer du code pour un schéma spécifique dans votre compte	Écrire	schema*		
PutResourcePolicy	Accorde l'autorisation d'attacher une politique basée sur des ressources à un registre donné	Écrire	registry*		
SearchSchemas	Accorde l'autorisation de rechercher des schémas en fonction de mots-clés spécifiés dans votre compte	List	schema*		
StartDiscoverer	Accorde l'autorisation de démarrer le détecteur spécifié. Une fois démarré, le détecteur enregistre automatiquement les schémas des événements publiés dans la source configurée dans votre compte	Écrire	discoverer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopDiscoverer	Accorde l'autorisation d'arrêter le détecteur spécifié. Une fois arrêté, le détecteur n'enregistrera plus les schémas des événements publiés vers la source configurée dans votre compte	Écrire	discoverer*		
TagResource	Accorde l'autorisation de baliser une ressource	Identification	discoverer		
			registry		
			schema		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	discoverer		
			registry		
			schema		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDiscoverer	Accorde l'autorisation de mettre à jour un détecteur existant dans votre compte	Écrire	discoverer*		
UpdateRegistry	Accorde l'autorisation de mettre à jour les métadonnées d'un registre existant dans votre compte	Écrire	registry*		
UpdateSchema	Accorde l'autorisation de mettre à jour un schéma existant dans votre compte	Écrire	schema*		

Types de ressources définis par Amazon EventBridge Schemas

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
discoverer	`arn:${Partition}:schemas:${Region}:${Account}:discoverer/${DiscovererId}`	aws:ResourceTag/${TagKey}
registry	`arn:${Partition}:schemas:${Region}:${Account}:registry/${RegistryName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
schema	`arn:${Partition}:schemas:${Region}:${Account}:schema/${RegistryName}/${SchemaName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon EventBridge Schemas

Amazon EventBridge Schemas définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des étiquettes	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le service d'injection de AWS défauts

AWS Le service d'injection de défauts (préfixe de service :`fis`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service d'injection de AWS défauts
- Types de ressources définis par le service d'injection de AWS défauts
- Clés de condition pour le service d'injection de AWS défauts

Actions définies par le service d'injection de AWS défauts

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExperimentTemplate	Autorise la création d'un AWS modèle d'expérience FIS	Écrire	action*		
			experiment-template*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateTargetAccountConfiguration	Accorde l'autorisation de créer une AWS configuration de compte cible FIS	Écrire	experiment-template*		
DeleteExperimentTemplate	Autorise la suppression du modèle d'expérience AWS FIS	Écrire	experiment-template*		
DeleteTargetAccountConfiguration	Accorde l'autorisation de supprimer une AWS configuration de compte cible FIS	Écrire	experiment-template*		
GetAction	Accorde l'autorisation de récupérer une AWS action FIS	Lecture	action*		
				aws:ResourceTag/${TagKey}	
GetExperiment	Autorise la récupération d'une AWS expérience FIS	Lecture	experiment*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExperimentTargetAccountConfiguration	Accorde l'autorisation de récupérer la configuration d'un compte cible AWS FIS pour une expérience AWS FIS	Lecture	experiment*		
GetExperimentTemplate	Autorise la récupération d'un AWS modèle d'expérience FIS	Lecture	experiment-template*		
				aws:ResourceTag/${TagKey}	
GetSafetyLever	Donne l'autorisation d'obtenir des informations sur le levier de sécurité	Lecture	safety-lever*		
GetTargetAccountConfiguration	Accorde l'autorisation de récupérer une configuration de compte cible AWS FIS pour un modèle d' AWS expérience FIS	Lecture	experiment-template*		
GetTargetResourceType	Accorde l'autorisation d'obtenir des informations sur le type de ressource spécifié	Lecture			
InjectApiInternalError [autorisation uniquement]	Accorde l'autorisation d'injecter une erreur interne d'API sur le AWS service fourni à partir d'une expérience FIS	Écrire	experiment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				fis:Service fis:Operations fis:Percentage fis:Targets	
InjectApiThrottleError [autorisation uniquement]	Accorde l'autorisation d'injecter une erreur d'accélération de l'API sur le AWS service fourni à partir d'une expérience FIS	Écrire	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InjectApiUnavailableError [autorisation uniquement]	Accorde l'autorisation d'injecter une erreur d'API non disponible sur le AWS service fourni à partir d'une expérience FIS	Écrire	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
ListActions	Permet de répertorier toutes les actions AWS FIS disponibles	List			
ListExperimentResolvedTargets	Donne l'autorisation de répertorier les cibles résolues pour les AWS expériences FIS	List	experiment*		
ListExperimentTargetAccountConfigurations	Permet de répertorier les configurations de comptes cibles pour les AWS expériences FIS	List	experiment*		
ListExperimentTemplates	Permet de répertorier tous les modèles d'expériences AWS FIS disponibles	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListExperiments	Donne l'autorisation de répertorier toutes les AWS expériences FIS disponibles	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une AWS ressource FIS	Lecture	action		
			experiment		
			experiment-template		
ListTargetAccountConfigurations	Accorde l'autorisation de répertorier les configurations de comptes cibles pour les AWS modèles d'expériences FIS	List	experiment-template*		
ListTargetResourceTypes	Accorde l'autorisation de répertorier les types de ressource	List			
StartExperiment	Donne l'autorisation de mener une AWS expérience FIS	Écrire	experiment*		iam:CreateServiceLinkedRole
			experiment-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
StopExperiment	Autorise l'arrêt d'une AWS expérience FIS	Écrire	experiment*		
TagResource	Accorde l'autorisation de baliser AWS les ressources FIS	Identification	action		
			experiment		
			experiment-template		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Autorise le débalisage des ressources AWS du FIS	Identification	action		
			experiment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			experiment-template		
				aws:TagKeys	
UpdateExperimentTemplate	Autorise la mise à jour du modèle d'expérience AWS FIS spécifié	Écrire	experiment-template*		
			action		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSafetyLeverState	Autorise la mise à jour de l'état du levier de sécurité	Écrire	safety-lever*		
UpdateTargetAccountConfiguration	Accorde l'autorisation de mettre à jour la AWS configuration d'un compte cible FIS	Écrire	experiment-template*		

Types de ressources définis par le service d'injection de AWS défauts

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
action	`arn:${Partition}:fis:${Region}:${Account}:action/${Id}`	aws:ResourceTag/${TagKey}
experiment	`arn:${Partition}:fis:${Region}:${Account}:experiment/${Id}`	aws:ResourceTag/${TagKey}
experiment-template	`arn:${Partition}:fis:${Region}:${Account}:experiment-template/${Id}`	aws:ResourceTag/${TagKey}
safety-lever	`arn:${Partition}:fis:${Region}:${Account}:safety-lever/${Id}`	

Clés de condition pour le service d'injection de AWS défauts

AWS Le service d'injection de défauts définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
fis:Operations	Filtre l'accès en fonction de la liste des opérations sur le AWS service concerné par l' AWS action FIS	ArrayOfString
fis:Percentage	Filtre l'accès en fonction du pourcentage d'appels concernés par l' AWS action FIS	Numérique
fis:Service	Filtre l'accès par le AWS service concerné par l' AWS action FIS	String
fis:Targets	Filtre l'accès en fonction de la liste des ressources ciblées ARNs par l' AWS action FIS	ArrayOfString

Actions, ressources et clés de condition pour Amazon FinSpace

Amazon FinSpace (préfixe de service :`finspace`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon FinSpace
- Types de ressources définis par Amazon FinSpace
- Clés de condition pour Amazon FinSpace

Actions définies par Amazon FinSpace

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConnectKxCluster [autorisation uniquement]	Accorde l'autorisation de se connecter à un cluster kdb	Écrire	kxCluster*		
CreateEnvironment	Accorde l'autorisation de créer un FinSpace environnement	Écrire	environment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxChangeset	Accorde l'autorisation de créer un jeu de modifications pour une base de données kdb	Écrire	kxDatabase*		
CreateKxCluster	Accorde l'autorisation de créer un cluster dans un environnement kdb géré	Écrire	kxCluster*		ec2:DescribeSubnets finspace:MountKxDatabase
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey}	
CreateKxDatabase	Accorde l'autorisation de créer une base de données kdb dans un environnement kdb géré	Écrire	kxDatabase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxDataview	Accorde l'autorisation de créer une vue de données dans un environnement kdb géré	Écrire	kxDataview*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxEnvironment	Accorde l'autorisation de créer un environnement kdb géré	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxScalingGroup	Accorde l'autorisation de créer un groupe Scaling dans un environnement kdb géré	Écrire	kxScalingGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxUser	Accorde l'autorisation de créer un utilisateur dans un environnement kdb géré	Écrire	kxEnvironment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxVolume	Accorde l'autorisation de créer un volume dans un environnement kdb géré	Écrire	kxVolume*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUser	Accorde l'autorisation de créer un FinSpace utilisateur	Écrire	environment*		
			user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEnvironment	Accorde l'autorisation de supprimer un FinSpace environnement	Écrire	environment*		
DeleteKxCluster	Accorde l'autorisation de supprimer un cluster kdb	Écrire	kxCluster*		
DeleteKxClusterNode	Accorde l'autorisation de supprimer un nœud d'un cluster kdb	Écrire	kxCluster*		
DeleteKxDatabase	Accorde l'autorisation de supprimer une base de données kdb	Écrire	kxDatabase*		
DeleteKxDataview	Accorde l'autorisation de supprimer une vue de données dans un environnement kdb géré	Écrire	kxDataview*		
DeleteKxEnvironment	Accorde l'autorisation de supprimer un environnement kdb géré	Écrire	kxEnvironment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteKxScalingGroup	Accorde l'autorisation de supprimer un groupe Scaling dans un environnement kdb géré	Écrire	kxScalingGroup*		
DeleteKxUser	Accorde l'autorisation de supprimer un utilisateur kdb	Écrire	kxUser*		
DeleteKxVolume	Accorde l'autorisation de supprimer un volume dans un environnement kdb géré	Écrire	kxVolume*		
GetEnvironment	Autorise la description d'un FinSpace environnement	Lecture	environment*		
GetKxChangeset	Accorde l'autorisation de décrire un jeu de modifications pour une base de données kdb	Lecture	kxDatabase*		
GetKxCluster	Accorde l'autorisation de décrire un cluster dans un environnement kdb géré	Lecture	kxCluster*		
GetKxConnectionString	Accorde l'autorisation de récupérer une chaîne de connexion pour les clusters kdb	Lecture	kxCluster*		finspace:ConnectKxCluster
GetKxDatabase	Accorde l'autorisation de décrire une base de données kdb	Lecture	kxDatabase*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetKxDataview	Accorde l'autorisation de décrire une vue de données dans un environnement kdb géré	Lecture	kxDataview*		
GetKxEnvironment	Accorde l'autorisation de décrire un environnement kdb géré	Lecture	kxEnvironment*		
GetKxScalingGroup	Accorde l'autorisation de décrire un groupe Scaling dans un environnement kdb géré	Lecture	kxScalingGroup*		
GetKxUser	Accorde l'autorisation de décrire un utilisateur kdb	Lecture	kxUser*		
GetKxVolume	Accorde l'autorisation de décrire un volume dans un environnement kdb géré	Lecture	kxVolume*		
GetLoadSampleDataSetGroupIntoEnvironmentStatus	Accorde l'autorisation de demander le statut de chargement de la solution groupée d'exemples de données	Lecture	environment*		
GetUser	Accorde l'autorisation de décrire un FinSpace utilisateur	Lecture	environment*		
			user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEnvironments	Accorde l'autorisation de répertorier FinSpace les environnements dans le Compte AWS	List	environment*		
ListKxChangesets	Accorde l'autorisation de répertorier les jeux de modifications pour une base de données kdb	List	kxDatabase*		
ListKxClusterNodes	Accorde l'autorisation de répertorier les nœuds de cluster dans un environnement kdb géré	List	kxCluster*		
ListKxClusters	Accorde l'autorisation de répertorier les clusters dans un environnement kdb géré	List	kxEnvironment*		
ListKxDatabases	Accorde l'autorisation de répertorier les bases de données kdb dans un environnement kdb géré	List	kxEnvironment*		
ListKxDataviews	Accorde l'autorisation de répertorier les vues de données d'une base de données	List	kxDatabase*		
ListKxEnvironments	Accorde l'autorisation de répertorier les environnements kdb gérés	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListKxScalingGroups	Accorde l'autorisation de répertorier des groupes Scaling dans un environnement kdb géré	List	kxEnvironment*		
ListKxUsers	Accorde l'autorisation de répertorier les utilisateurs dans un environnement kdb géré	List	kxEnvironment*		
ListKxVolumes	Accorde l'autorisation de répertorier les volumes dans un environnement kdb géré	List	kxEnvironment*		
ListTagsForResource	Accorde l'autorisation de renvoyer une liste d'étiquettes pour une ressource	List	environment*		
			kxCluster*		
			kxDatabase*		
			kxDataview*		
			kxEnvironment*		
			kxScalingGroup*		
			kxUser*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			kxVolume*		
ListUsers	Accorde l'autorisation de répertorier FinSpace les utilisateurs dans un environnement	List	environment*		
			user*		
LoadSampleDataSetGroupIntoEnvironment	Autorise le chargement d'un exemple de bundle de données dans votre FinSpace environnement	Écrire	environment*		
MountKxDatabase [autorisation uniquement]	Accorde l'autorisation de monter une base de données sur un cluster kdb	Écrire	kxDatabase*		
ResetUserPassword	Accorde l'autorisation de réinitialiser le mot de passe d'un FinSpace utilisateur	Écrire	environment*		
			user*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	environment		
			kxCluster		
			kxDatabase		
			kxDataview		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			kxEnvironment		
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			kxUser		
			kxVolume		
				aws:TagKeys	
UpdateEnvironment	Autorise la mise à jour d'un FinSpace environnement	Écrire	environment*		
UpdateKxClusterCodeConfiguration	Accorde l'autorisation de mettre à jour la configuration du code d'un cluster dans un environnement kdb géré	Écrire	kxCluster*		
UpdateKxClusterDatabases	Accorde l'autorisation de mettre à jour les bases de données d'un cluster dans un environnement kdb géré	Écrire	kxCluster*		
UpdateKxDatabase	Accorde l'autorisation de mettre à jour une base de données kdb	Écrire	kxDatabase*		
UpdateKxDataview	Accorde l'autorisation de mettre à jour une vue de données dans un environnement kdb géré	Écrire	kxDataview*		
UpdateKxEnvironment	Accorde l'autorisation de mettre à jour un environnement kdb géré	Écrire	kxEnvironment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateKxEnvironmentNetwork	Accorde l'autorisation de mettre à jour le réseau d'un environnement kdb géré	Écrire	kxEnvironment*		
UpdateKxUser	Accorde l'autorisation de mettre à jour un utilisateur kdb	Écrire	kxUser*		
UpdateKxVolume	Accorde l'autorisation de mettre à jour un volume dans un environnement kdb géré	Écrire	kxVolume*		
UpdateUser	Accorde l'autorisation de mettre à jour un FinSpace utilisateur	Écrire	environment*		
			user*		

Types de ressources définis par Amazon FinSpace

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
environment	`arn:${Partition}:finspace:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
user	arn:${Partition}:finspace:${Region}:${Account}:user/${UserId}	aws:ResourceTag/${TagKey}
kxEnvironment	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}	aws:ResourceTag/${TagKey}
kxUser	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxUser/${UserName}	aws:ResourceTag/${TagKey}
kxCluster	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxCluster/${KxCluster}	aws:ResourceTag/${TagKey}
kxDatabase	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}	aws:ResourceTag/${TagKey}
kxScalingGroup	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxScalingGroup/${KxScalingGroup}	aws:ResourceTag/${TagKey}
kxDataview	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}/kxDataview/${KxDataview}	aws:ResourceTag/${TagKey}
kxVolume	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxVolume/${KxVolume}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon FinSpace

Amazon FinSpace définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour l' FinSpace API Amazon

FinSpace L'API Amazon (préfixe de service :`finspace-api`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l' FinSpace API Amazon

- Types de ressources définis par l' FinSpace API Amazon
- Clés de condition pour FinSpace l'API Amazon

Actions définies par l' FinSpace API Amazon

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProgrammaticAccessCredentials	Accorde l'autorisation de récupérer les informations d'accès FinSpace programmatiques	Lecture	credential*		

Types de ressources définis par l' FinSpace API Amazon

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
credential	`arn:${Partition}:finspace-api:${Region}:${Account}:/credentials/programmatic`	

Clés de condition pour FinSpace l'API Amazon

FinSpace L'API ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Firewall Manager

AWS Firewall Manager (préfixe de service :`fms`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Firewall Manager
- Types de ressources définis par AWS Firewall Manager
- Clés de condition pour AWS Firewall Manager

Actions définies par AWS Firewall Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAdminAccount	Accorde l'autorisation de définir le compte administrateur de AWS Firewall Manager et active le service dans tous les comptes de l'organisation	Écrire			
AssociateThirdPartyFirewall	Accorde l'autorisation de définir l'administrateur Firewall Manager en tant qu'administrateur locataire d'un service de pare-feu tiers	Écrire			
BatchAssociateResource	Accorde l'autorisation d'associer des ressources à un ensemble de ressources AWS Firewall Manager	Écrire	resource-set*		
BatchDisassociateResource	Accorde l'autorisation de dissocier les ressources d'un ensemble de ressources AWS Firewall Manager	Écrire	resource-set*		
DeleteAppsList	Accorde l'autorisation de supprimer définitivement une liste d'applications AWS Firewall Manager	Écrire	applications-list*		
DeleteNotificationChannel	Accorde l'autorisation de supprimer une association AWS Firewall Manager avec le rôle IAM et la rubrique	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Amazon Simple Notification Service (SNS) utilisée pour informer l'administrateur FM des principaux événements et erreurs FM au sein de l'organisation				
DeletePolicy	Accorde l'autorisation de supprimer définitivement une politique de AWS Firewall Manager	Écrire	policy*		
				aws:ResourceTag/${TagKey}	
DeleteProtocolsList	Accorde l'autorisation de supprimer définitivement une liste de protocoles AWS Firewall Manager	Écrire	protocols-list*		
DeleteResourceSet	Accorde l'autorisation de supprimer définitivement un ensemble de ressources AWS Firewall Manager	Écrire	resource-set*		
				aws:ResourceTag/${TagKey}	
DisassociateAdminAccount	Accorde l'autorisation de dissocier le compte défini comme compte administrateur de AWS Firewall Manager et désactive le service dans tous les comptes de l'organisation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateThirdPartyFirewall	Accorde l'autorisation de dissocier un administrateur Firewall Manager d'un locataire de pare-feu tiers	Écrire			
GetAdminAccount	Accorde l'autorisation de renvoyer le compte AWS Organizations associé à AWS Firewall Manager en tant qu'administrateur de AWS Firewall Manager	Lecture			
GetAdminScope	Accorde l'autorisation de renvoyer des informations sur la portée administrative du compte spécifié	Lecture			
GetAppsList	Accorde l'autorisation de renvoyer des informations sur la liste d'applications AWS Firewall Manager spécifiée	Lecture	applications-list*		
GetComplianceDetail	Accorde l'autorisation de récupérer des informations détaillées de conformité sur le compte de membre spécifié Ces informations détaillées incluent les ressources conformes et non conformes à la politique spécifiée.	Lecture	policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetNotificationChannel	Accorde l'autorisation de récupérer des informations relatives à la rubrique Amazon Simple Notification Service (SNS) utilisée pour enregistrer les journaux SNS de Firewall Manager AWS	Lecture			
GetPolicy	Accorde l'autorisation de récupérer des informations relatives à la politique de AWS Firewall Manager spécifiée	Lecture	policy*		
GetProtectionStatus	Permet de récupérer les informations récapitulatives des attaques au niveau des politiques en cas d'attaque DDo S potentielle	Lecture	policy*		
GetProtocolsList	Accorde l'autorisation de renvoyer des informations sur la liste de protocoles AWS Firewall Manager spécifiée	Lecture	protocols-list*		
GetResourceSet	Accorde l'autorisation de récupérer des informations sur le jeu de ressources AWS Firewall Manager spécifié	Lecture	resource-set*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetThirdPartyFirewallAssociationStatus	Accorde l'autorisation de récupérer le statut d'onboarding d'un compte administrateur Firewall Manager au locataire d'un fournisseur de pare-feu tiers	Lecture			
GetViolationDetails	Accorde l'autorisation de récupérer les violations pour une ressource en fonction de la politique de AWS Firewall Manager spécifiée et Compte AWS	Lecture	policy*		
ListAdminAccountsForOrganization	Accorde l'autorisation de renvoyer un AdminAccounts objet répertoriant les administrateurs de Firewall Manager au sein de l'organisation qui ont été intégrés à Firewall Manager par Associate AdminAccount	List			
ListAdminsManagingAccount	Accorde l'autorisation de répertorier les comptes qui gèrent le compte membre AWS d'Organizations spécifié	List			
ListAppsLists	Accorde l'autorisation de renvoyer un tableau d'AppsListDataSummary objets	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListComplianceStatus	Accorde l'autorisation de récupérer un tableau d' PolicyComplianceStatus objets dans la réponse. PolicyComplianceStatus À utiliser pour obtenir un résumé des comptes de membres protégés par la politique spécifiée	List	policy*		
ListDiscoveredResources	Accorde l'autorisation de récupérer un tableau de ressources dans les comptes de l'organisation pouvant être associées à un ensemble de ressources	List			
ListMemberAccounts	Accorde l'autorisation de récupérer un tableau d'ID de compte membre si le mandataire est le compte d'administrateur FMS	List			
ListPolicies	Accorde l'autorisation de récupérer un tableau d' PolicySummary objets dans la réponse	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProtocolsLists	Accorde l'autorisation de renvoyer un tableau d' ProtocolsListDataSummary objets	List			
ListResourceSetResources	Accorde l'autorisation de récupérer un tableau de ressources associées à un ensemble de ressources	List	resource-set*		
ListResourceSets	Accorde l'autorisation de récupérer un tableau d' ResourceSetSummary objets	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource donnée	Lecture	policy*		
ListThirdPartyFirewallFirewallPolicies	Accorde l'autorisation de récupérer une liste de toutes les politiques de pare-feu tiers associées au compte de l'administrateur du pare-feu tiers	List			
PutAdminAccount	Accorde l'autorisation de créer ou de mettre à jour un compte administrateur de Firewall Manager	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutAppsList	Accorde l'autorisation de créer une liste d'applications AWS Firewall Manager	Écrire	applications-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutNotificationChannel	Accorde l'autorisation de désigner le rôle IAM et la rubrique Amazon Simple Notification Service (SNS) que AWS Firewall Manager (FM) pourrait utiliser pour informer l'administrateur FM des principaux événements et erreurs FM survenus au sein de l'organisation	Écrire			
PutPolicy	Accorde l'autorisation de créer une politique AWS Firewall Manager	Écrire	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutProtocolsList	Accorde l'autorisation de créer une liste de protocoles AWS Firewall Manager	Écrire	protocols-list*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
PutResourceSet	Accorde l'autorisation de créer un ensemble de ressources AWS Firewall Manager	Écrire	resource-set*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource donnée	Balisage	applications-list		
			policy		
			protocols-list		
			resource-set		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource donnée	Identification	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:TagKeys	

Types de ressources définis par AWS Firewall Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
policy	arn:${Partition}:fms:${Region}:${Account}:policy/${Id}	aws:ResourceTag/${TagKey}
applications-list	arn:${Partition}:fms:${Region}:${Account}:applications-list/${Id}	aws:ResourceTag/${TagKey}
protocols-list	arn:${Partition}:fms:${Region}:${Account}:protocols-list/${Id}	aws:ResourceTag/${TagKey}
resource-set	arn:${Partition}:fms:${Region}:${Account}:resource-set/${Id}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Firewall Manager

AWS Firewall Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la requête	ArrayOfString

Actions, ressources et clés de condition pour Amazon Forecast

Amazon Forecast (préfixe de service : `forecast`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Forecast
- Types de ressources définis par Amazon Forecast
- Clés de condition pour Amazon Forecast

Actions définies par Amazon Forecast

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAutoPredictor	Accorde l'autorisation de créer un prédicteur automatique.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataset	Accorde l'autorisation de créer un jeu de données.	Écriture	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetGroup	Accorde l'autorisation de créer un groupe de jeux de données.	Écriture	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetImportJob	Accorde l'autorisation de créer une tâche d'importation d'un jeu de données.	Écrire	datasetImportJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainability	Accorde l'autorisation de créer une explicabilité	Écrire	forecast*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainabilityExport	Accorde l'autorisation de créer une exportation d'explicabilité à l'aide d'une ressource d'explicabilité	Écrire	explainability*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecast	Accorde l'autorisation de créer une prévision.	Écrire	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateForecastEndpoint [autorisation uniquement]	Accorde l'autorisation de créer un point de terminaison à l'aide d'une ressource Predictor	Écrire	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastExportJob	Accorde l'autorisation de créer une tâche d'exportation de prévision à l'aide d'une ressource de prévision.	Écrire	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMonitor	Accorde l'autorisation de créer un moniteur à l'aide d'une ressource Predictor	Écrire	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictor	Accorde l'autorisation de créer un prédicteur.	Écriture	datasetGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictorBacktestExportJob	Accorde l'autorisation de créer une tâche d'exportation du rétro-test du prédicteur à l'aide d'un prédicteur.	Écrire	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfAnalysis	Accorde l'autorisation de créer une analyse par simulation	Écrire	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecast	Accorde l'autorisation de créer une prévision par simulation	Écrire	whatIfAnalysis*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecastExport	Accorde l'autorisation de créer une tâche d'exportation de prévision par simulation à l'aide d'une ressource de prévision par simulation	Écrire	whatIfForecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données.	Écriture	dataset*		
DeleteDatasetGroup	Accorde l'autorisation de supprimer un groupe de jeux de données.	Écriture	datasetGroup*		
DeleteDatasetImportJob	Accorde l'autorisation de supprimer une tâche d'importation d'un jeu de données.	Écrire	datasetImportJob*		
DeleteExplainability	Accorde l'autorisation de supprimer une explicabilité	Écrire	explainability*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteExplainabilityExport	Accorde l'autorisation de supprimer une exportation d'explicabilité	Écrire	explainabilityExport*		
DeleteForecast	Accorde l'autorisation de supprimer une prévision.	Écrire	forecast*		
DeleteForecastEndpoint [autorisation uniquement]	Accorde l'autorisation de supprimer une ressource de point de terminaison	Écrire	endpoint*		
DeleteForecastExportJob	Accorde l'autorisation de supprimer une tâche d'exportation de prévision.	Écrire	forecastExport*		
DeleteMonitor	Accorde l'autorisation de supprimer une ressource de moniteur	Écrire	monitor*		
DeletePredictor	Accorde l'autorisation de supprimer un prédicteur.	Écriture	predictor*		
DeletePredictorBacktestExportJob	Accorde l'autorisation de supprimer une tâche d'exportation rétro-test du prédicteur.	Écriture	predictorBacktestExportJob*		
DeleteResourceTree	Accorde l'autorisation de supprimer une ressource et ses ressources enfants	Écrire	dataset*		
			datasetGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			whatIfForecastExport*		
DeleteWhatIfAnalysis	Accorde l'autorisation de supprimer une analyse par simulation	Écrire	whatIfAnalysis*		
DeleteWhatIfForecast	Accorde l'autorisation de supprimer une prévision par simulation	Écrire	whatIfForecast*		
DeleteWhatIfForecastExport	Accorde l'autorisation de supprimer une exportation de prévision par simulation	Écrire	whatIfForecastExport*		
DescribeAutoPredictor	Accorde l'autorisation de décrire un prédicteur automatique.	Lecture	predictor*		
DescribeDataset	Accorde l'autorisation de décrire un jeu de données.	Lecture	dataset*		
DescribeDatasetGroup	Accorde l'autorisation de décrire un groupe de jeux de données.	Lecture	datasetGroup*		
DescribeDatasetImportJob	Accorde l'autorisation de décrire une tâche d'importation d'un jeu de données.	Lecture	datasetImportJob*		
DescribeExplainability	Accorde l'autorisation de décrire une explicabilité	Lecture	explainability*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeExplainabilityExport	Accorde l'autorisation de décrire une exportation d'explicabilité	Lecture	explainabilityExport*		
DescribeForecast	Accorde l'autorisation de décrire une prévision.	Lecture	forecast*		
DescribeForecastEndpoint [autorisation uniquement]	Accorde l'autorisation de décrire une ressource de point de terminaison	Lecture	endpoint*		
DescribeForecastExportJob	AuAccorde l'autorisation de décrire une tâche d'exportation de prévision.	Lecture	forecastExport*		
DescribeMonitor	Accorde l'autorisation de décrire une ressource de moniteur	Lecture	monitor*		
DescribePredictor	Accorde l'autorisation de décrire un prédicteur.	Lecture	predictor*		
DescribePredictorBacktestExportJob	Accorde l'autorisation de décrire une tâche d'exportation du rétro-test du prédicteur.	Lecture	predictorBacktestExportJob*		
DescribeWhatIfAnalysis	Accorde l'autorisation de décrire une analyse par simulation	Lecture	whatIfAnalysis*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWhatIfForecast	Accorde l'autorisation de décrire une prévision par simulation	Lecture	whatIfForecast*		
DescribeWhatIfForecastExport	Accorde l'autorisation de décrire une exportation de prévision par simulation	Lecture	whatIfForecastExport*		
GetAccuracyMetrics	Accorde l'autorisation d'obtenir des métriques de précision pour un prédicteur.	Lecture	predictor*		
GetRecentForecastContext [autorisation uniquement]	Accorde l'autorisation d'obtenir le contexte de prévision d'une série chronologique pour un point de terminaison	Lecture	endpoint*		
InvokeForecastEndpoint [autorisation uniquement]	Accorde l'autorisation d'appeler le point de terminaison pour obtenir des prévisions pour une série chronologique	Lecture	endpoint*		
ListDatasetGroups	Accorde l'autorisation de répertorier tous les groupes de jeux de données.	Lecture			
ListDatasetImportJobs	Accorde l'autorisation de répertorier toutes les tâches d'importation de jeux de données.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDatasets	Accorde l'autorisation de répertorier tous les jeux de données.	Lecture			
ListExplainabilities	Accorde l'autorisation de répertorier toutes les explicabilités.	Lecture			
ListExplainabilityExports	Accorde l'autorisation de répertorier toutes les exportations d'explicabilité.	Lecture			
ListForecastExportJobs	Accorde l'autorisation de répertorier toutes les tâches d'exportation de prévision.	Lecture			
ListForecasts	Accorde l'autorisation de répertorier toutes les prévisions.	Lecture			
ListMonitorEvaluations	Accorde l'autorisation de répertorier tous les résultats de l'évaluation d'un moniteur.	Lecture	monitor*		
ListMonitors	Accorde l'autorisation de répertorier toutes les ressources du moniteur	Lecture			
ListPredictorBacktestExportJobs	Accorde l'autorisation de répertorier toutes les tâches d'exportation du rétro-test du prédicteur.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPredictors	Accorde l'autorisation de répertorier tous les prédicteurs.	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource Amazon Forecast.	Lecture	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
ListWhatIfAnalyses	Accorde l'autorisation de répertorier toutes les analyses par simulation	Lecture			
ListWhatIfForecastExports	Accorde l'autorisation de répertorier toutes les exportations de prévisions par simulation	Lecture			
ListWhatIfForecasts	Accorde l'autorisation de répertorier toutes les prévisions par simulation	Lecture			
QueryForecast	Accorde l'autorisation de récupérer une prévision pour un seul article.	Lecture	forecast*		
QueryWhatIfForecast	Accorde l'autorisation de récupérer une prévision par simulation pour un seul article	Lecture	whatIfForecast*		
ResumeResource		Écrire	monitor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de reprendre les tâches liées aux ressources Amazon Forecast			aws:RequestTag/${TagKey} aws:TagKeys	
StopResource	Accorde l'autorisation d'arrêter les tâches liées aux ressources Amazon Forecast	Écriture	datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation d'associer les balises spécifiées à une ressource.	Balisage	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées pour une ressource.	Balisage	dataset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			whatIfForecastExport		
				aws:TagKeys	
UpdateDatasetGroup	Accorde l'autorisation de mettre à jour un groupe de jeux de données.	Écriture	dataset*		
			datasetGroup*		

Types de ressources définis par Amazon Forecast

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
dataset	`arn:${Partition}:forecast:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
datasetGroup	`arn:${Partition}:forecast:${Region}:${Account}:dataset-group/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
datasetImportJob	arn:${Partition}:forecast:${Region}:${Account}:dataset-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
algorithm	arn:${Partition}:forecast:::algorithm/${ResourceId}	
predictor	arn:${Partition}:forecast:${Region}:${Account}:predictor/${ResourceId}	aws:ResourceTag/${TagKey}
predictorBacktestExportJob	arn:${Partition}:forecast:${Region}:${Account}:predictor-backtest-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
forecast	arn:${Partition}:forecast:${Region}:${Account}:forecast/${ResourceId}	aws:ResourceTag/${TagKey}
forecastExport	arn:${Partition}:forecast:${Region}:${Account}:forecast-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
explainability	arn:${Partition}:forecast:${Region}:${Account}:explainability/${ResourceId}	aws:ResourceTag/${TagKey}
explainabilityExport	arn:${Partition}:forecast:${Region}:${Account}:explainability-export/${ResourceId}	aws:ResourceTag/${TagKey}
monitor	arn:${Partition}:forecast:${Region}:${Account}:monitor/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfAnalysis	arn:${Partition}:forecast:${Region}:${Account}:what-if-analysis/${ResourceId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
whatIfForecast	arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfForecastExport	arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast-export/${ResourceId}	aws:ResourceTag/${TagKey}
endpoint	arn:${Partition}:forecast:${Region}:${Account}:forecast-endpoint/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Forecast

Amazon Forecast définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Fraud Detector

Amazon Fraud Detector (préfixe de service : `frauddetector`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Fraud Detector
- Types de ressources définis par Amazon Fraud Detector
- Clés de condition pour Amazon Fraud Detector

Actions définies par Amazon Fraud Detector

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchCreateVariable	Accorde l'autorisation de créer un lot de variables.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetVariable	Accorde l'autorisation d'obtenir un lot de variables.	List	variable*		
CancelBatchImportJob	Accorde l'autorisation d'annuler la tâche d'importation par lots spécifiée.	Écrire	batch-import*		
CancelBatchPredictionJob	Accorde l'autorisation d'annuler la tâche de prédiction par lots spécifiée.	Écrire	batch-prediction*		
CreateBatchImportJob	Accorde l'autorisation de créer une tâche d'importation par lots	Écrire	batch-import*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBatchPredictionJob	Accorde l'autorisation de créer une tâche de prédiction par lots.	Écriture	batch-prediction*		
			detector*		
			detector-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorVersion	Accorde l'autorisation de créer une version de détecteur. La version de détecteur démarre à l'état DRAFT.	Écrire	detector*		
			external-model		
			model-version		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateList	Autorise la création d'un studio.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateModel	Accorde l'autorisation de créer un modèle à l'aide du type de modèle spécifié.	Écriture	event-type*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelVersion	Accorde l'autorisation de créer une version du modèle à l'aide du type et de l'ID de modèle spécifiés.	Écriture	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRule	Accorde l'autorisation de créer une règle à utiliser avec le détecteur spécifié.	Écriture	detector*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateVariable	Accorde l'autorisation de créer une variable.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBatchImportJob	Accorde l'autorisation de supprimer une tâche d'importation par lots	Écrire	batch-import*		
DeleteBatchPredictionJob	Accorde l'autorisation de supprimer une tâche de prédiction par lots.	Écriture	batch-prediction*		
DeleteDetector	Accorde l'autorisation de supprimer le détecteur . Avant de supprimer un détecteur, vous devez d'abord supprimer toutes les versions de détecteur et toutes les versions de règle associées au détecteur.	Écriture	detector*		
DeleteDetectorVersion	Accorde l'autorisation de supprimer la version de détecteur. Vous ne pouvez pas supprimer les versions de détecteur qui sont dans l'état ACTIVE.	Écriture	detector-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEntityType	Accorde l'autorisation de supprimer un type d'entité. Vous ne pouvez pas supprimer un type d'entité inclus dans un type d'événement.	Écriture	entity-type*		
DeleteEvent	Accorde l'autorisation de supprimer l'événement spécifié.	Écriture	event-type*		
DeleteEventType	Accorde l'autorisation de supprimer un type d'événement. Vous ne pouvez pas supprimer un type d'événement utilisé dans un détecteur ou un modèle.	Écrire	event-type*		
DeleteEventsByEventType	Accorde l'autorisation de supprimer les événements pour le type d'événement spécifié	Écrire	event-type*		
DeleteExternalModel	Autorise le retrait d'un SageMaker modèle d'Amazon Fraud Detector. Vous pouvez supprimer un SageMaker modèle Amazon s'il n'est pas associé à une version de détecteur	Écrire	external-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLabel	Accorde l'autorisation de supprimer une étiquette. Vous ne pouvez pas supprimer les étiquettes incluses dans un type d'événement dans Amazon Fraud Detector. Vous ne pouvez pas supprimer une étiquette affectée à un ID d'événement. Vous devez d'abord supprimer l'ID d'événement correspondant.	Écrire	label*		
DeleteList	Accorde l'autorisation de supprimer une vague	Écrire	list*		
				aws:ResourceTag/${TagKey}	
DeleteModel	Accorde l'autorisation de supprimer un modèle. Vous pouvez supprimer des modèles et des versions de modèles dans Amazon Fraud Detector à condition qu'ils ne soient pas associés à une version de détecteur.	Écriture	model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteModelVersion	Accorde l'autorisation de supprimer une version de modèle. Vous pouvez supprimer des modèles et des versions de modèles dans Amazon Fraud Detector à condition qu'ils ne soient pas associés à une version de détecteur.	Écriture	model-version*		
DeleteOutcome	Accorde l'autorisation de supprimer un résultat. Vous ne pouvez pas supprimer un résultat qui est utilisé dans une version de règle.	Écriture	outcome*		
DeleteRule	Accorde l'autorisation de supprimer la règle. Vous ne pouvez pas supprimer une règle si elle est utilisée par une version de détecteur ACTIVE ou INACTIVE.	Écriture	rule*		
DeleteVariable	Accorde l'autorisation de supprimer une variable. Vous ne pouvez pas supprimer les variables qui sont incluses dans un type d'événement dans Amazon Fraud Detector.	Écriture	variable*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDetector	Accorde l'autorisation d'obtenir toutes les versions d'un détecteur spécifié.	Lecture	detector*		
DescribeModelVersions	Accorde l'autorisation d'obtenir toutes les versions de modèle pour le type de modèle spécifié ou pour le type de modèle et l'ID de modèle spécifiés. Vous pouvez également obtenir des détails pour une seule version de modèle spécifié.	Lecture	model-version		
GetBatchImportJobValidationReport [autorisation uniquement]	Octroie l'autorisation d'obtenir le rapport de validation des données d'une tâche d'importation par lots spécifique	Lecture	batch-import*		
GetBatchImportJobs	Accorde l'autorisation d'obtenir toutes les tâches d'importation par lots ou une tâche spécifique si vous spécifiez un ID de tâche	List	batch-import		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBatchPredictionJobs	Accorde l'autorisation d'obtenir toutes les tâches de prédiction par lots ou une tâche spécifique si vous spécifiez un ID de tâche. Il s'agit d'une API paginée. Si vous fournissez un maxResults null, cette action récupère un maximum de 50 enregistrements par page. Si vous fournissez un maxResults, la valeur doit être comprise entre 1 et 50. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination fourni dans le GetBatchPredictionJobsResponse cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	List	batch-prediction		
GetDeleteEventsByEventTypeStatus	Accorde l'autorisation d'obtenir le statut d'exécution de l'DeleteEventsByEventType API d'un type d'événement spécifique	Lecture	event-type*		
GetDetectorVersion	Accorde l'autorisation d'obtenir une version de détecteur particulière.	Lecture	detector-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDetectors	Accorde l'autorisation d'obtenir tous les détecteurs ou un seul détecteur si un identifiant de détecteur est spécifié. Il s'agit d'une API paginée. Si vous fournissez un maxResults null, cette action récupère un maximum de 10 enregistrements par page. Si vous fournissez un maxResults, la valeur doit être comprise entre 5 et 10. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination fourni dans le GetDetectorsResponse cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	Liste	detector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEntityTypes	Accorde l'autorisation d'obtenir tous les types d'entité ou un type d'entité spécifique si un nom est spécifié. Il s'agit d'une API paginée. Si vous fournissez un maxResults null, cette action récupère un maximum de 10 enregistrements par page. Si vous fournissez un maxResults, la valeur doit être comprise entre 5 et 10. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination fourni dans le GetEntityTypesResponse cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	List	entity-type		
GetEvent	Accorde l'autorisation d'obtenir les détails de l'évènement spécifié	Lecture	event-type*		
GetEventPrediction	Accorde l'autorisation d'évaluer un événement par rapport à une version de détecteur. Si aucun ID de version n'est fourni, la version (ACTIVE) du détecteur est utilisée	Lecture	detector*		
			detector-version*		
			event-type*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEventPrediction Metadata	Accorde l'autorisation d'obtenir des détails supplémentaires relatifs à une prédiction en particulier	Lecture	detector*		
			detector-version*		
			event-type*		
GetEventTypes	Accorde l'autorisation d'obtenir tous les types d'événements ou un type d'événement spécifique si un nom est fourni. Il s'agit d'une API paginée. Si vous fournissez un maxResults null, cette action récupère un maximum de 10 enregistrements par page. Si vous fournissez un maxResults, la valeur doit être comprise entre 5 et 10. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination fourni dans le GetEventTypesResponse cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	List	event-type		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExternalModels	Accorde l'autorisation d'obtenir les informations relatives à un ou plusieurs SageMaker modèles Amazon importés dans le service. Il s'agit d'une API paginée. Si vous fournissez un élément maxResults null, cette action récupère un maximum de 10 enregistrements par page. Si vous fournissez un maxResults, la valeur doit être comprise entre 5 et 10. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination fourni dans le GetExternalModelsResult cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	Liste	external-model		
GetKMSEncryptionKey	Accorde l'autorisation d'obtenir la clé de chiffrement si une clé principale client (CMK) Key Management Service (KMS) a été spécifiée pour être utilisée afin de chiffrer le contenu dans Amazon Fraud Detector.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLabels	Accorde l'autorisation d'obtenir toutes les étiquettes ou une étiquette spécifique si un nom est fourni. Il s'agit d'une API paginée. Si vous fournissez un maxResults null, cette action récupère un maximum de 50 enregistrements par page. Si vous fournissez un maxResults, la valeur doit être comprise entre 10 et 50. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination fourni dans le GetGetLabelsResponse cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	List	label		
GetListElements	Accorde l'autorisation d'obtenir une liste de jeux de données	Lecture	list*		
				aws:ResourceTag/${TagKey}	
GetListsMetadata	Accorde l'autorisation d'obtenir des métadonnées des listes	List	list		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetModelVersion	Accorde l'autorisation d'obtenir les détails de la version de modèle spécifié.	Lecture	model-version*		
GetModels	Accorde l'autorisation d'obtenir un ou plusieurs modèles. Obtient tous les modèles pour le Compte AWS cas où aucun type de modèle et aucun identifiant de modèle ne sont fournis. Obtient tous les modèles pour le type de modèle Compte AWS et, si le type de modèle est spécifié mais que l'identifiant du modèle n'est pas fourni. Obtient un modèle spécifique si le tuple (type de modèle, ID de modèle) est spécifié.	Liste	model		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOutcomes	Accorde l'autorisation d'obtenir un ou plusieurs résultats. Il s'agit d'une API paginée. Si vous fournissez un élément maxResults null, cette action récupère un maximum de 100 enregistrements par page. Si vous fournissez un maxResults, la valeur doit être comprise entre 50 et 100. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination fourni dans le GetOutcomesResult cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	Liste	outcome		
GetRules	Accorde l'autorisation d'obtenir toutes les règles d'un détecteur (paginé) si RuleID et RuleVersion ne sont pas spécifiés. Obtient toutes les règles pour le détecteur et le RuleID s'il est présent (paginé). Obtient une règle spécifique si RuleID et RuleVersion sont spécifiés.	Liste	rule		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetVariables	Accorde l'autorisation d'obtenir toutes les variables ou la variable spécifique. Il s'agit d'une API paginée. Si vous fournissez une maxSizePer page nulle, vous pouvez récupérer un maximum de 100 enregistrements par page. Si vous indiquez maxSizePer Page, la valeur doit être comprise entre 50 et 100. Pour obtenir le résultat de la page suivante, fournissez un jeton de pagination dans GetVariablesResult le cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	List	variable		
ListEvent Predictions	Accorde l'autorisation d'obtenir une liste des prévisions passées	List	detector		
			detector-version		
			event-type		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises associées à la ressource. Il s'agit d'une API paginée. Pour obtenir les résultats de la page suivante, fournissez le jeton de pagination de la réponse dans le cadre de votre demande. Un jeton de pagination nul récupère les enregistrements depuis le début.	Lecture	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDetector	Accorde l'autorisation de créer ou de mettre à jour un détecteur.	Écriture	detector*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutEntityType	Accorde l'autorisation de créer ou de mettre à jour un type d'entité. Une entité représente qui exécute l'événement. Dans le cadre d'une prévision de fraude, vous transmettez l'ID d'entité pour indiquer l'entité spécifique qui a exécuté l'événement. Un type d'entité classe l'entité. Les exemples de classifications incluent le client, le vendeur ou le compte.	Écriture	entity-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutEventType	Accorde l'autorisation de créer ou de mettre à jour un type d'événement. Un événement est une activité commerciale évaluée pour le risque de fraude. Avec Amazon Fraud Detector, vous générez des prédictions de fraude pour les événements. Un type d'événement définit la structure d'un événement envoyé à Amazon Fraud Detector. Cela inclut les variables envoyées dans le cadre de l'événement, l'entité exécutant l'événement (par exemple, un client) et les étiquettes qui classent l'événement. Les exemples de types d'événements incluent les transactions de paiement en ligne, les enregistrements de compte et les authentifications.	Écrire	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutExternalModel	Accorde l'autorisation de créer ou de mettre à jour un point de terminaison SageMaker modèle Amazon. Vous pouvez également utiliser cette action pour mettre à jour la configuration du point de terminaison du modèle, y compris le rôle IAM et and/or les variables mappées.	Écrire	event-type*		
			external-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutKMSEncryptionKey	Accorde l'autorisation de spécifier la clé principale client (CMK) KMS (Key Management Service) à utiliser pour chiffrer le contenu dans Amazon Fraud Detector.	Écriture			
PutLabel	Accorde l'autorisation de créer ou de mettre à jour l'étiquette. Une étiquette classe un événement comme frauduleux ou légitime. Les étiquettes sont associées à des types d'événements et sont utilisées pour entraîner des modèles de machine learning supervisés dans Amazon Fraud Detector.	Écriture	label*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutOutcome	Accorde l'autorisation de créer ou de mettre à jour un résultat.	Écrire	outcome*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SendEvent	Accorde l'autorisation d'envoyer un événement	Écrire	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation d'affecter des balises à une ressource.	Balisage	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Balisage	batch-import		
			batch-prediction		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDetectorVersion	Accorde l'autorisation de mettre à jour une version de détecteur. Les attributs de version du détecteur que vous pouvez mettre à jour incluent les modèles, les points de terminaison de modèle externes, les règles et la description. Vous ne pouvez mettre à jour qu'une version de détecteur à l'état DRAFT.	Écriture	detector*		
			external-model		
			model-version		
UpdateDetectorVersionMetadata	Accorde l'autorisation de mettre à jour la description de la version de détecteur . Vous pouvez mettre à jour les métadonnées de n'importe quelle version de détecteur (DRAFT, ACTIVE ou INACTIVE).	Écrire	detector-version*		
UpdateDetectorVersionStatus	Accorde l'autorisation de mettre à jour le statut de la version du détecteur. Vous pouvez effectuer les promotions ou rétrogradations suivantes en utilisant UpdateDetectorVersionStatus : BROUILLON à ACTIF, ACTIF à INACTIF et INACTIF à ACTIF	Écrire	detector-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEventLabel	Accorde l'autorisation de mettre à jour la valeur du label d'un enregistrement d'événement existant	Écrire	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateList	Accorde l'autorisation de mettre à jour un studio.	Écrire	list*		
				aws:ResourceTag/${TagKey}	
UpdateModel	Accorde l'autorisation de mettre à jour un modèle. Cette action vous permet de mettre à jour l'attribut de description.	Écriture	model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateModelVersion	Accorde l'autorisation de mettre à jour une version de modèle. La mise à jour d'une version de modèle entraîne une nouvelle version de modèle existante à l'aide de données de formation mises à jour et produit une nouvelle version mineure du modèle. Vous pouvez mettre à jour l'emplacement du jeu de données de formation et les attributs de rôle d'accès aux données à l'aide de cette action. Cette action crée et entraîne une nouvelle version mineure du modèle, par exemple la version 1.01, 1.02, 1.03.	Écriture	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateModelVersionStatus	Accorde l'autorisation de mettre à jour l'état d'une version de modèle.	Écriture	model-version*		
UpdateRuleMetadata	Accorde l'autorisation de mettre à jour les métadonnées d'une règle. L'attribut de description peut être mis à jour.	Écriture	rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRuleVersion	Accorde l'autorisation de mettre à jour une version de règle, ce qui produit une nouvelle version de règle. Met à jour une version de règle, ce qui produit une nouvelle version de règle (version 1, 2, 3...).	Écriture	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVariable	Accorde l'autorisation de mettre à jour une variable.	Écriture	variable*		

Types de ressources définis par Amazon Fraud Detector

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
batch-prediction	`arn:${Partition}:frauddetector:${Region}:${Account}:batch-prediction/${ResourcePath}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
detector	arn:${Partition}:frauddetector:${Region}:${Account}:detector/${ResourcePath}	aws:ResourceTag/${TagKey}
detector-version	arn:${Partition}:frauddetector:${Region}:${Account}:detector-version/${ResourcePath}	aws:ResourceTag/${TagKey}
entity-type	arn:${Partition}:frauddetector:${Region}:${Account}:entity-type/${ResourcePath}	aws:ResourceTag/${TagKey}
external-model	arn:${Partition}:frauddetector:${Region}:${Account}:external-model/${ResourcePath}	aws:ResourceTag/${TagKey}
event-type	arn:${Partition}:frauddetector:${Region}:${Account}:event-type/${ResourcePath}	aws:ResourceTag/${TagKey}
label	arn:${Partition}:frauddetector:${Region}:${Account}:label/${ResourcePath}	aws:ResourceTag/${TagKey}
model	arn:${Partition}:frauddetector:${Region}:${Account}:model/${ResourcePath}	aws:ResourceTag/${TagKey}
model-version	arn:${Partition}:frauddetector:${Region}:${Account}:model-version/${ResourcePath}	aws:ResourceTag/${TagKey}
outcome	arn:${Partition}:frauddetector:${Region}:${Account}:outcome/${ResourcePath}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
rule	arn:${Partition}:frauddetector:${Region}:${Account}:rule/${ResourcePath}	aws:ResourceTag/${TagKey}
variable	arn:${Partition}:frauddetector:${Region}:${Account}:variable/${ResourcePath}	aws:ResourceTag/${TagKey}
batch-import	arn:${Partition}:frauddetector:${Region}:${Account}:batch-import/${ResourcePath}	aws:ResourceTag/${TagKey}
list	arn:${Partition}:frauddetector:${Region}:${Account}:list/${ResourcePath}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Fraud Detector

Amazon Fraud Detector définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction des balises qui sont transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des balises associées à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction des clés de balise qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le niveau AWS gratuit

AWS Le niveau gratuit (préfixe de service :`freetier`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Free Tier
- Types de ressources définis par AWS Free Tier
- Clés de condition pour le niveau AWS gratuit

Actions définies par AWS Free Tier

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountActivity	Accorde l'autorisation d'obtenir un enregistrement d'activité spécifique	Lecture			
GetAccountPlanState	Accorde l'autorisation d'obtenir toutes les informations	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	relatives à l'état du plan de compte lié au niveau gratuit				
GetFreeTierAlertPreference [autorisation uniquement]	Accorde l'autorisation d'obtenir la préférence d'alerte de l'offre gratuite (par adresse e-mail)	Lecture			
GetFreeTierUsage	Accorde l'autorisation d'obtenir les limites d'utilisation et le statut d'utilisation depuis le début du mois (MTD) de l'offre gratuite	Lecture			
ListAccountActivities	Accorde l'autorisation de répertorier les activités disponibles	List			
PutFreeTierAlertPreference [autorisation uniquement]	Accorde l'autorisation de définir les préférences d'alerte de l'offre gratuite (par adresse e-mail)	Écrire			
UpgradeAccountPlan	Accorde l'autorisation de déclencher une mise à niveau du plan de compte	Écrire			

Types de ressources définis par AWS Free Tier

AWS Free Tier ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Free Tier, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le niveau AWS gratuit

Free Tier ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon FreeRTOS

Amazon FreeRTOS (préfixe de service : `freertos`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon FreeRTOS
- Types de ressources définis par Amazon FreeRTOS
- Clés de condition pour Amazon FreeRTOS

Actions définies par Amazon FreeRTOS

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSoftwareConfiguration	Accorde l'autorisation de créer une configuration logicielle	Écrire	configuration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Accorde l'autorisation de créer une abonnement au plan de maintenance étendue (EMP) de FreeRTOS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSoftwareConfiguration	Accorde l'autorisation de supprimer la configuration logicielle	Écrire	configuration*		
DescribeHardwarePlatform	Accorde l'autorisation de décrire la plateforme matérielle	Lecture			
DescribeSoftwareConfiguration	Accorde l'autorisation de décrire la configuration logicielle	Lecture	configuration*		
DescribeSubscription	Accorde l'autorisation de décrire l'abonnement pour le	Lecture	subscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	plan de maintenance étendue (EMP) de FreeRTOS				
GetEmpPatchUrl	Accorde l'autorisation d'obtenir l'URL des versions de correctif, des différences de correctif et des notes de publication des logiciels dans le cadre du plan de maintenance étendue (EMP) de FreeRTOS	Lecture			
GetSoftwareURL	Accorde l'autorisation d'obtenir l'URL de téléchargement du logiciel Amazon FreeRTOS	Lecture			
GetSoftwareURLForConfiguration	Accorde l'autorisation d'obtenir l'URL de téléchargement du logiciel Amazon FreeRTOS en fonction de la configuration	Lecture			
GetSubscriptionBillingAmount	Accorde l'autorisation de récupérer le montant de la facturation de l'abonnement pour le plan de maintenance étendue (EMP) de FreeRTOS	Lecture			
ListFreeRTOSVersions	Accorde l'autorisation de répertorier les versions de AmazonFree RTOS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListHardwarePlatforms	Accorde l'autorisation de répertorier les plateformes matérielles	List			
ListHardwareVendors	Accorde l'autorisation de répertorier les fournisseurs de matériel	List			
ListSoftwareConfigurations	Accorde l'autorisation de supprimer les configurations logicielles	List			
ListSoftwarePatches	Accorde l'autorisation de créer un abonnement au plan de maintenance étendue (EMP) de FreeRTOS	List			
ListSubscriptionEmails	Accorde l'autorisation de répertorier les e-mails d'abonnement au plan de maintenance étendue (EMP) de FreeRTOS	List			
ListSubscriptions	Accorde l'autorisation de répertorier les abonnements au plan de maintenance étendue (EMP) de FreeRTOS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEmailRecipients	Accorde l'autorisation de mettre à jour la liste des e-mails d'abonnement au plan de maintenance étendue (EMP) de FreeRTOS	Écrire			
UpdateSoftwareConfiguration	Accorde l'autorisation de mettre à jour la configuration logicielle	Écrire	configuration*		
VerifyEmail	Accorde l'autorisation de vérifier l'e-mail pour le plan de maintenance étendue (EMP) de FreeRTOS	Écrire			

Types de ressources définis par Amazon FreeRTOS

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
configuration	`arn:${Partition}:freertos:${Region}:${Account}:configuration/${ConfigurationName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
subscription	`arn:${Partition}:freertos:${Region}:${Account}:subscription/${SubscriptionID}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon FreeRTOS

Amazon FreeRTOS définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé de balise présente dans la demande que l'utilisateur envoie à Amazon FreeRTOS	String
aws:ResourceTag/${TagKey}	Filtre l'accès par tag (composant clé associé à une ressource Amazon FreeRTOS)	String
aws:TagKeys	Filtre l'accès en fonction de la liste de tous les noms de clés de balise associés à la ressource dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon FSx

Amazon FSx (préfixe de service :`fsx`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon FSx
- Types de ressources définis par Amazon FSx
- Clés de condition pour Amazon FSx

Actions définies par Amazon FSx

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateFileGateway [autorisation uniquement]	Accorde l'autorisation d'associer une instance de File Gateway à un système de fichiers Amazon FSx pour Windows File Server	Écrire	file-system*		
AssociateFileSystemAliases	Accorde l'autorisation d'associer des alias DNS à un système de fichiers Amazon FSx pour Windows File Server	Écrire	file-system*		
BypassSnaplockEnterpriseRetention	Accorde l'autorisation d'autoriser la suppression d'un volume FSx destiné à ONTAP SnapLock Enterprise	Gestion des autorisations	volume*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]	contenant des fichiers WORM (écriture unique, lecture multiple) avec des périodes de rétention actives				
CancelDataRepositoryTask	Accorde l'autorisation d'annuler une tâche liée à un référentiel de données	Écriture	task*		
CopyBackup	Accorde l'autorisation de copier une sauvegarde.	Écrire	backup*		fsx:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshotAndUpdateVolume	Autorise la mise à jour d'un volume existant à l'aide d'un instantané provenant d'un autre système de fichiers Amazon FSx pour OpenZFS	Écrire	snapshot*		
			volume*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAndAttachS3AccessPoint	Accorde l'autorisation de créer et d'associer un point d'accès S3 à un système de FSx fichiers	Écrire	volume		s3:CreateAccessPoint s3:GetAccessPoint s3:PutAccessPointPolicy
CreateBackup	Autorise la création d'une nouvelle sauvegarde d'un système de FSx fichiers Amazon ou d'un FSx volume Amazon	Écrire	backup*		fsx:TagResource
			file-system		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataRepositoryAssociation	Accorde l'autorisation de créer une nouvelle association de référentiel de données pour un système de fichiers Amazon FSx for Lustre	Écrire	association*	fsx:NfsDataRepositoryAuthenticationEnabled fsx:NfsDataRepositoryEncryptionInTransitEnabled	fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryTask	Accorde l'autorisation de créer une nouvelle tâche de référentiel de données pour un système de fichiers Amazon FSx for Lustre	Écrire	file-system*		fsx:TagResource
			task*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFileCache	Accorde l'autorisation de créer un cache de fichiers Amazon vide	Écrire	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	Accorde l'autorisation de créer un nouveau système de FSx fichiers Amazon vide	Écrire	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	Autorise la création d'un nouveau système de FSx fichiers Amazon à partir d'une sauvegarde existante	Écrire	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Accorde l'autorisation de créer un instantané sur un volume	Écrire	snapshot*		fsx:TagResource
			volume*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageVirtualMachine	Accorde l'autorisation de créer une nouvelle machine virtuelle de stockage dans un système de fichiers Amazon FSx for Ontap	Écrire	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	Accorde l'autorisation de créer un volume	Écrire	volume*		fsx:TagResource
			snapshot		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	Accorde l'autorisation de créer un volume à partir d'une sauvegarde	Écrire	backup*		fsx:TagResource
			storage-virtual-machine*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBackup	Accorde l'autorisation de supprimer une sauvegarde, en supprimant son contenu. Après la suppression, la sauvegarde n'existe plus, et ses données ne sont plus disponibles.	Écrire	backup*		
DeleteDataRepositoryAssociation	Accorde l'autorisation de supprimer une association liée à un référentiel de données.	Écrire	association*		
DeleteFileCache	Accorde l'autorisation de supprimer un cache de fichiers, en supprimant son contenu	Écrire	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFileSystem	Accorde l'autorisation de supprimer un système de fichiers, en supprimant son contenu et toutes les sauvegardes automatiques existantes du système de fichiers	Écrire	file-system*		fsx:CreateBackup fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de gérer le partage de FSx volumes entre comptes via AWS Resource Access Manager (RAM). PutResourcePolicy et GetResourcePolicy sont également obligatoires	Gestion des autorisations	volume*		
DeleteSnapshot	Accorde l'autorisation de supprimer un instantané sur un volume	Écrire	snapshot*		
DeleteStorageVirtualMachine	Accorde l'autorisation de supprimer une machine virtuelle de stockage, en supprimant son contenu.	Écrire	storage-virtual-machine*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteVolume	Accorde l'autorisation de supprimer un volume, en supprimant son contenu et toutes les sauvegardes automatiques existantes du volume	Écrire	volume*		fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways [autorisation uniquement]	Accorde l'autorisation de décrire les instances de File Gateway associées à un système de fichiers Amazon FSx pour Windows File Server	Lecture	file-system*		
DescribeBackups	Accorde l'autorisation de renvoyer les descriptions de toutes les sauvegardes que vous détenez Compte AWS dans le Région AWS terminal que vous appelez	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDataRepositoryAssociations	Accorde l'autorisation de renvoyer les descriptions de toutes les associations de référentiels Région AWS de données que vous détenez Compte AWS dans le terminal que vous appelez	Lecture			
DescribeDataRepositoryTasks	Accorde l'autorisation de renvoyer les descriptions de toutes les tâches du référentiel Région AWS de données qui vous appartiennent Compte AWS dans le terminal que vous appelez	Lecture			
DescribeFileCaches	Accorde l'autorisation de renvoyer les descriptions de tous les caches de fichiers que vous détenez Compte AWS dans le Région AWS terminal que vous appelez	Lecture			
DescribeFileSystemAliases	Autorise le renvoi de la description de tous les alias DNS détenus par votre système de fichiers Amazon FSx pour Windows File Server	Lecture	file-system*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFileSystems	Accorde l'autorisation de renvoyer les descriptions de tous les systèmes Région AWS de fichiers que vous possédez Compte AWS dans le terminal que vous appelez	Lecture			
DescribeS3AccessPointAttachments	Autorise le renvoi des descriptions des pièces jointes aux points d'accès S3	Lecture			
DescribeSharedVpcConfiguration	Accorde l'autorisation de renvoyer des descriptions indiquant si les mises à jour des tables de FSx routage à partir des comptes des participants sont autorisées dans votre compte	Lecture			
DescribeSnapshots	Accorde l'autorisation de renvoyer les descriptions de tous les instantanés que vous détenez Compte AWS dans le Région AWS terminal que vous appelez	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeStorageVirtualMachines	Accorde l'autorisation de renvoyer les descriptions de toutes les machines virtuelles Région AWS de stockage que vous détenez Compte AWS dans le terminal que vous appelez	Lecture			
DescribeVolumes	Accorde l'autorisation de renvoyer les descriptions de tous les volumes que vous détenez Compte AWS dans le Région AWS terminal que vous appelez	Lecture			
DetachAndDeleteS3AccessPoint	Accorde l'autorisation de détacher un point d'accès S3 d'un système de FSx fichiers Amazon et de supprimer le point d'accès S3	Écrire	volume		s3:DeleteAccessPoint
DisassociateFileGateway [autorisation uniquement]	Accorde l'autorisation de dissocier une instance de File Gateway d'un système de fichiers Amazon FSx pour Windows File Server	Écrire	file-system*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateFileSystemAliases	Accorde l'autorisation de dissocier les alias de système de fichiers d'un système de fichiers Amazon FSx pour Windows File Server	Écrire	file-system*		
GetResourcePolicy [autorisation uniquement]	Accorde l'autorisation de gérer le partage de FSx volumes entre comptes via AWS Resource Access Manager (RAM). PutResourcePolicy et DeleteResourcePolicy sont également obligatoires	Gestion des autorisations	volume*		
ListTagsForResource	Accorde l'autorisation de répertorier les tags d'une FSx ressource Amazon	Lecture	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ManageBackupPrincipalAssociations [autorisation uniquement]	Accorde l'autorisation de gérer les associations principales de AWS sauvegarde via Backup	Gestion des autorisations	backup*		
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de gérer le partage de FSx volumes entre comptes via AWS Resource Access Manager (RAM). DeleteResourcePolicy et GetResourcePolicy sont également obligatoires	Gestion des autorisations	volume*		
ReleaseFileSystemNfsV3Locks	Accorde l'autorisation de libérer les verrous NFS V3 du système de fichiers	Écrire	file-system*		
RestoreVolumeFromSnapshot	Accorde l'autorisation de restaurer l'état du volume à partir d'un instantané	Écrire	snapshot* volume*		
StartMisconfiguredStateRecovery	Accorde l'autorisation de démarrer la récupération d'un état mal configuré	Écrire	file-system*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser une FSx ressource Amazon	Identification	association	fsx:NfsDataRepositoryAuthenticationEnabled fsx:NfsDataRepositoryEncryptionInTransitEnabled	
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			volume	fsx:ParentVolumeId fsx:StorageVirtualMachineId	
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer un tag d'une FSx ressource Amazon	Identification	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateDataRepositoryAssociation	Accorde l'autorisation de mettre à jour la configuration d'association liée à un référentiel de données	Écrire	association*		
UpdateFileCache	Accorde l'autorisation de mettre à jour la configuration du cache de fichiers	Écrire	file-cache*		
UpdateFileSystem	Accorde l'autorisation de mettre à jour la configuration du système de fichiers	Écrire	file-system*		
UpdateSharedVpcConfiguration	Accorde l'autorisation d'activer ou de désactiver les mises à jour des tables de FSx routage à partir des comptes des participants de votre compte	Écrire			
UpdateSnapshot	Accorde l'autorisation de mettre à jour une configuration d'instantané	Écrire	snapshot*		
UpdateStorageVirtualMachine	Accorde l'autorisation de mettre à jour la configuration de la machine virtuelle de stockage	Écrire	storage-virtual-machine*		
UpdateVolume		Écrire	volume*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de mettre à jour la configuration des volumes			fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Types de ressources définis par Amazon FSx

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> Amazon FSx pour Windows File Server, Lustre et Ontap partagent certains des mêmes types de ressources, avec le même format ARN pour chacun.

Types de ressources	ARN	Clés de condition
file-system	`arn:${Partition}:fsx:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
file-cache	`arn:${Partition}:fsx:${Region}:${Account}:file-cache/${FileCacheId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
backup	arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}	aws:ResourceTag/${TagKey}
storage-virtual-machine	arn:${Partition}:fsx:${Region}:${Account}:storage-virtual-machine/${FileSystemId}/${StorageVirtualMachineId}	aws:ResourceTag/${TagKey}
task	arn:${Partition}:fsx:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}
association	arn:${Partition}:fsx:${Region}:${Account}:association/${FileSystemIdOrFileCacheId}/${DataRepositoryAssociationId}	aws:ResourceTag/${TagKey}
volume	arn:${Partition}:fsx:${Region}:${Account}:volume/${FileSystemId}/${VolumeId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:fsx:${Region}:${Account}:snapshot/${VolumeId}/${SnapshotId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon FSx

Amazon FSx définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
fsx:IsBackupCopyDestination	Filtre l'accès selon que la sauvegarde est une sauvegarde de destination pour une CopyBackup opération	Booléen
fsx:IsBackupCopySource	Filtre l'accès selon que la sauvegarde est une sauvegarde source pour une CopyBackup opération	Booléen
fsx:NfsDataRepositoryAuthenticationEnabled	Filtre l'accès en fonction des référentiels de données NFS qui prennent en charge l'authentification	Booléen
fsx:NfsDataRepositoryEncryptionInTransitEnabled	Filtre l'accès par les référentiels de données NFS qui prennent en charge encryption-in-transit	Booléen
fsx:ParentVolumeId	Filtre l'accès en fonction du volume parent contenant pour la mutation des opérations de volume	String
fsx:StorageVirtualMachineId	Filtre l'accès en fonction de la machine virtuelle de stockage contenant pour un volume pour la mutation des opérations de volume	String

Actions, ressources et clés de condition pour les GameLift serveurs Amazon

Amazon GameLift Servers (préfixe de service :`gamelift`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les GameLift serveurs Amazon
- Types de ressources définis par les GameLift serveurs Amazon
- Clés de condition pour les GameLift serveurs Amazon

Actions définies par les GameLift serveurs Amazon

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptMatch	Autorise le joueur à enregistrer l'acceptation ou le rejet d'un FlexMatch match proposé	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ClaimGameServer	Accorde l'autorisation de localiser et de réserver un serveur de jeu pour héberger une nouvelle session de jeu	Écriture	gameServerGroup*		
CreateAlias	Accorde l'autorisation de définir un nouvel alias pour une flotte	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateBuild	Accorde l'autorisation de créer une nouvelle génération de jeu à l'aide de fichiers stockés dans un compartiment Amazon S3	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateContainerFleet	Accorde l'autorisation de créer un nouveau parc de conteneurs de ressources informatiques pour faire fonctionner vos serveurs de jeu	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole
CreateContainerGroupDefinition	Accorde l'autorisation de créer une nouvelle définition de groupe de conteneurs à l'aide d'images stockées dans un référentiel Amazon ECR	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer gamelift:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFleet	Accorde l'autorisation de créer une nouvelle flotte de ressources informatiques pour exécuter vos serveurs de jeu	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole
CreateFleetLocations	Accorde l'autorisation de spécifier des emplacements supplémentaires pour une flotte	Écriture	containerFleet		ec2:DescribeAvailabilityZones ec2:DescribeRegions
			fleet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGameServerGroup	Accorde l'autorisation de créer un nouveau groupe de serveurs de jeu, de configurer un groupe Auto Scaling correspondant et de lancer les instances sur les serveurs de jeu hôtes	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	autoscaling:CreateAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:PutLifecycleHook autoscaling:PutScalingPolicy ec2:DescribeAvailabilityZones ec2:DescribeSubnets events:PutRule

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					events:PutTargets gamelift:TagResource iam:PassRole
CreateGameSession	Accorde l'autorisation de démarrer une nouvelle session de jeu sur une flotte spécifiée	Écriture			
CreateGameSessionQueue	Accorde l'autorisation de configurer une nouvelle file d'attente pour le traitement des demandes de placement de session de jeu	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateLocation	Accorde l'autorisation de définir un nouvel emplacement pour une flotte	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMatchmakingConfiguration	Accorde l'autorisation de créer un nouveau FlexMatch système de matchmaking	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateMatchmakingRuleSet	Accorde l'autorisation de créer une nouvelle règle de matchmaking définie pour FlexMatch	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreatePlayerSession	Accorde l'autorisation de réserver un créneau de session de jeu disponible pour un joueur	Écriture			
CreatePlayerSessions	Accorde l'autorisation de réserver des créneaux de session de jeu disponibles pour plusieurs joueurs	Écriture			
CreateScript	Accorde l'autorisation de créer un script Serveurs en temps réel	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateVpcPeeringAuthorization	Accorde l'autorisation de GameLift créer ou de supprimer une connexion de peering entre un VPC de GameLift flotte et un VPC d'un autre Compte AWS	Écrire			ec2:AcceptVpcPeeringConnection ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateRoute ec2:DeleteRoute ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:RevokeSecurityGroupEgress

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:RevokeSecurityGroupIngress
CreateVpcPeeringConnection	Autorise l'établissement d'une connexion de peering entre le VPC de votre GameLift flotte et un VPC d'un autre compte	Écrire			
DeleteAlias	Accorde l'autorisation de supprimer un alias	Écriture	alias*		
DeleteBuild	Accorde l'autorisation de supprimer une génération de jeu	Écrire	build*		
DeleteContainerFleet	Autorise la suppression d'une flotte de conteneurs	Écrire	containerFleet*		
DeleteContainerGroupDefinition	Autorise la suppression d'une définition de groupe de conteneurs	Écrire	containerGroupDefinition*		
DeleteFleet	Accorde l'autorisation de supprimer une flotte vide	Écriture	fleet*		
DeleteFleetLocations	Accorde l'autorisation de supprimer des emplacements pour une flotte	Écriture	containerFleet		
			fleet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteGameServerGroup	Accorde l'autorisation de supprimer définitivement un groupe de serveurs de jeux et d'arrêter l'activité FleetIQ pour le groupe Auto Scaling correspondant	Écriture	gameServerGroup*		autoscaling:DeleteAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:ExitStandby autoscaling:ResumeProcesses autoscaling:SetInstanceProtection autoscaling:UpdateAutoScalingGroup
DeleteGameSessionQueue	Accorde l'autorisation de supprimer une file d'attente de session de jeu existante	Écrire	gameSessionQueue*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLocation	Accorde l'autorisation de supprimer un emplacement	Écrire	location*		
DeleteMatchmakingConfiguration	Accorde l'autorisation de supprimer un FlexMatch matchmaker existant	Écrire	matchmakingConfiguration*		
DeleteMatchmakingRuleSet	Accorde l'autorisation de supprimer un ensemble de règles FlexMatch de matchmaking existant	Écrire	matchmakingRuleSet*		
DeleteScalingPolicy	Accorde l'autorisation de supprimer un ensemble de règles de scalabilité automatique	Écriture	containerFleet		
			fleet		
DeleteScript	Accorde l'autorisation de supprimer un script Serveurs en temps réel	Écriture	script*		
DeleteVpcPeeringAuthorization	Accorde l'autorisation d'annuler une autorisation d'appairage de VPC	Écrire			
DeleteVpcPeeringConnection	Accorde l'autorisation de supprimer une connexion de peering entre VPCs	Écrire			
DeregisterCompute	Accorde l'autorisation d'annuler l'enregistrement d'un calcul par rapport à une flotte	Écrire	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterGameServer	Accorde l'autorisation de supprimer un serveur de jeu d'un groupe de serveurs de jeux	Écriture	gameServerGroup*		
DescribeAlias	Accorde l'autorisation de récupérer les propriétés d'un alias	Lecture	alias*		
DescribeBuild	Accorde l'autorisation de récupérer les propriétés d'une génération de jeu	Lecture	build*		
DescribeCompute	Accorde l'autorisation de récupérer des informations pour un calcul dans une flotte	Lecture	containerFleet		
			fleet		
DescribeContainerFleet	Permet de récupérer les propriétés d'une flotte de conteneurs existante	Lecture	containerFleet*		
DescribeContainerGroupDefinition	Accorde l'autorisation de récupérer les propriétés d'une définition de groupe de conteneurs existante	Lecture	containerGroupDefinition*		
DescribeEC2InstanceLimits	Accorde l'autorisation de récupérer l'utilisation maximale autorisée et actuelle pour les types d'instance EC2	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFleetAttributes	Accorde l'autorisation de récupérer des propriétés générales, y compris le statut, des flottes	Lecture			
DescribeFleetCapacity	Accorde l'autorisation de récupérer les paramètres de capacité actuels pour les flottes gérées	Lecture			
DescribeFleetDeployment	Accorde l'autorisation de récupérer les propriétés d'un déploiement de flotte existant	Lecture	containerFleet*		
DescribeFleetEvents	Accorde l'autorisation de récupérer les entrées du journal des événements d'une flotte	Lecture	containerFleet		
			fleet		
DescribeFleetLocationAttributes	Accorde l'autorisation de récupérer les propriétés générales, y compris les statuts, des emplacements d'une flotte	Lecture	containerFleet		
			fleet		
DescribeFleetLocationCapacity	Accorde l'autorisation de récupérer le paramètre de capacité actuel pour l'emplacement d'une flotte	Lecture	containerFleet		
			fleet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFleetLocationUtilization	Accorde l'autorisation de récupérer les statistiques d'utilisation pour l'emplacement d'une flotte	Lecture	fleet*		
DescribeFleetPortSettings	Accorde l'autorisation de récupérer les autorisations de connexion entrante pour une flotte	Lecture	fleet*		
DescribeFleetUtilization	Accorde l'autorisation de récupérer les statistiques d'utilisation pour les flottes	Lecture			
DescribeGameServer	Accorde l'autorisation de récupérer les propriétés d'un serveur de jeu	Lecture	gameServerGroup*		
DescribeGameServerGroup	Accorde l'autorisation de récupérer les propriétés d'un groupe de serveurs de jeux	Lecture	gameServerGroup*		
DescribeGameServerInstances	Accorde l'autorisation de récupérer le statut des instances EC2 dans un groupe de serveurs de jeux	Lecture	gameServerGroup*		
DescribeGameSessionDetails	Accorde l'autorisation de récupérer les propriétés des sessions de jeu dans une flotte, y compris la politique de protection	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGameSessionPlacement	Accorde l'autorisation de récupérer les détails d'une demande de placement de session de jeu	Lecture			
DescribeGameSessionQueues	Accorde l'autorisation de récupérer les propriétés des files d'attente de session de jeu	Lecture			
DescribeGameSessions	Accorde l'autorisation de récupérer les propriétés des sessions de jeux dans une flotte	Lecture			
DescribeInstances	Accorde l'autorisation de récupérer des informations sur les instances d'un parc géré	Lecture	containerFleet fleet		
DescribeMatchmaking	Accorde l'autorisation de récupérer des détails des tickets de mise en relation	Lecture			
DescribeMatchmakingConfigurations	Autorise les FlexMatch matchmakers à récupérer des propriétés	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeMatchmakingRuleSets	Accorde l'autorisation de récupérer les propriétés des ensembles FlexMatch de règles de matchmaking	Lecture			
DescribePlayerSessions	Accorde l'autorisation de récupérer les propriétés des sessions de joueur dans une session de jeu	Lecture			
DescribeRuntimeConfiguration	Accorde l'autorisation de récupérer la configuration d'exécution actuelle d'une flotte	Lecture	fleet*		
DescribeScalingPolicies	Accorde l'autorisation de récupérer toutes les stratégies de mise à l'échelle appliquées à une flotte	Lecture	containerFleet		
			fleet		
DescribeScript	Accorde l'autorisation de récupérer les propriétés d'un script Serveurs en temps réel	Lecture	script*		
DescribeVpcPeeringAuthorizations	Accorde l'autorisation de récupérer les autorisations d'appairage de VPC valides	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeVpcPeeringConnections	Accorde l'autorisation de récupérer les détails sur les connexions d'appairage VPC actives ou en attente	Lecture			
GetComputeAccess	Accorde l'autorisation de récupérer les informations d'identification pour accéder à distance à un ordinateur dans un parc géré	Lecture	containerFleet		
			fleet		
GetComputeAuthToken	Accorde l'autorisation de récupérer un jeton d'authentification qui permet aux processus d'un ordinateur d'envoyer des demandes au GameLift service Amazon	Lecture	containerFleet		
			fleet		
GetGameSessionLogUrl	Accorde l'autorisation de récupérer l'emplacement des journaux stockés pour une session de jeu	Lecture			
GetInstanceAccess	Accorde l'autorisation de demander l'accès distant à une instance de flotte spécifiée	Lecture	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPlayerConnectionDetails	Accorde l'autorisation de récupérer les points de connexion des joueurs et les jetons de passerelle des joueurs pour une session de jeu	Lecture			
ListAliases	Accorde l'autorisation de récupérer tous les alias définis dans la région actuelle	Liste			
ListBuilds	Accorde l'autorisation de récupérer toutes les générations de jeux dans la région actuelle	List			
ListCompute	Accorde l'autorisation de récupérer toutes les ressources de calcul dans la région actuelle	List	containerFleet		
			fleet		
ListContainerFleets	Accorde l'autorisation de récupérer les propriétés de toutes les flottes de conteneurs existantes dans la région actuelle	List			
ListContainerGroupDefinitionVersions	Accorde l'autorisation de récupérer les propriétés de toutes les versions d'une définition de groupe de conteneurs existante	List	containerGroupDefinition*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListContainerGroupDefinitions	Accorde l'autorisation de récupérer les propriétés de toutes les définitions de groupes de conteneurs existantes dans la région actuelle	List			
ListFleetDeployments	Accorde l'autorisation de récupérer les propriétés de tous les déploiements de flotte existants dans la région actuelle	List			
ListFleets	Permet de récupérer une liste des flottes de toutes IDs les flottes de la région actuelle	List			
ListGameServerGroups	Accorde l'autorisation de récupérer tous les groupes de serveurs de jeux définis dans la région actuelle	Liste			
ListGameServers	Accorde l'autorisation de récupérer tous les serveurs de jeux en cours d'exécution dans un groupe de serveurs de jeux	List	gameServerGroup*		
ListLocations	Accorde l'autorisation de récupérer tous les emplacements dans ce compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListScripts	Accorde l'autorisation de récupérer les propriétés de tous les scripts Serveurs en temps réel dans la région actuelle	List			
ListTagsForResource	Accorde l'autorisation de récupérer des balises pour les GameLift ressources	Lecture	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			script		
PutScalingPolicy	Accorde l'autorisation de créer ou de mettre à jour une politique de scalabilité automatique de la flotte	Écrire	containerFleet		
			fleet		
RegisterCompute	Accorde l'autorisation d'enregistrer un calcul par rapport à une flotte	Écrire	fleet*		
RegisterGameServer	Autorise FleetIQ à avertir GameLift FleetIQ lorsqu'un nouveau serveur de jeu est prêt à héberger le jeu	Écrire	gameServerGroup*		
RequestUploadCredentials	Accorde l'autorisation de récupérer les nouvelles informations d'identification de chargement à utiliser lors du chargement d'une nouvelle génération de jeu	Lecture	build*		
ResolveAlias	Accorde l'autorisation de récupérer l'ID de flotte associé à un alias	Lecture	alias*		
ResumeGameServerGroup	Accorde l'autorisation de rétablir l'activité FleetIQ suspendue pour un groupe de serveurs de jeux	Écriture	gameServerGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchGameSessions	Accorde l'autorisation de récupérer les sessions de jeux correspondant à un ensemble de critères de recherche	Lecture			
StartFleetActions	Autorise la reprise de l'activité d'auto-scaling sur une flotte après sa suspension avec StopFleetActions ()	Écrire	containerFleet fleet		
StartGameSessionPlacement	Accorde l'autorisation d'envoyer une demande de placement de session de jeu à une file d'attente de session de jeu	Écrire	gameSessionQueue*		
StartMatchBackfill	Accorde l'autorisation de demander le FlexMatch matchmaking pour occuper les places disponibles dans une session de jeu existante	Écrire			
StartMatchmaking	Accorde l'autorisation de demander le FlexMatch matchmaking pour un ou un groupe de joueurs et de lancer le placement d'une session de jeu	Écrire			
StopFleetActions	Accorde l'autorisation de suspendre l'activité de scalabilité automatique sur une flotte	Écriture	containerFleet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			fleet		
StopGameSessionPlacement	Accorde l'autorisation dl'annuler une demande de placement de session de jeu en cours	Écriture			
StopMatchmaking	Accorde l'autorisation d'annuler une demande de mise en relation ou de renvoi de correspondance en cours	Écriture			
SuspendGameServerGroup	Accorde l'autorisation d'arrêter temporairement l'activité FleetIQ pour un groupe de serveurs de jeux	Écrire	gameServerGroup*		
TagResource	Accorde l'autorisation de baliser GameLift les ressources	Identification	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateGameSession	Autorise l'arrêt d'une session de jeu existante	Écrire			
UntagResource	Accorde l'autorisation de supprimer le balisage des ressources GameLift	Identification	alias		
			build		
			containerFleet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:TagKeys	
UpdateAlias	Accorde l'autorisation de mettre à jour les propriétés d'un alias existant	Écriture	alias*		
UpdateBuild	Accorde l'autorisation de mettre à jour les métadonnées d'une génération existante	Écrire	build*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateContainerFleet	Autorise la mise à jour d'une flotte de conteneurs existante	Écrire	containerFleet*		
UpdateContainerGroupDefinition	Autorise la mise à jour des propriétés d'une définition de groupe de conteneurs existante	Écrire	containerGroupDefinition*		ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer
UpdateFleetAttributes	Accorde l'autorisation de mettre à jour les propriétés générales d'une flotte existante	Écrire	fleet*		
UpdateFleetCapacity	Accorde l'autorisation d'ajuster les paramètres de capacité d'une flotte gérée	Écrire	containerFleet fleet		
UpdateFleetPortSettings	Accorde l'autorisation de régler les paramètres de port d'une flotte	Écriture	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGameServer	Accorde l'autorisation de modifier les propriétés, l'état de santé ou le statut d'utilisation du serveur de jeu	Écriture	gameServerGroup*		
UpdateGameServerGroup	Accorde l'autorisation de mettre à jour les propriétés du groupe de serveurs de jeu, y compris les types d'instance autorisés	Écriture	gameServerGroup*		iam:PassRole
UpdateGameSession	Accorde l'autorisation de mettre à jour les propriétés d'une session de jeu existante	Écriture			
UpdateGameSessionQueue	Accorde l'autorisation de mettre à jour les propriétés d'une file d'attente de session de jeu existante	Écrire	gameSessionQueue*		
UpdateMatchmakingConfiguration	Accorde l'autorisation de mettre à jour les propriétés d'une configuration FlexMatch de matchmaking existante	Écrire	matchmakingConfiguration*		
UpdateRuntimeConfiguration	Accorde l'autorisation de mettre à jour la configuration des processus serveur sur les instances d'une flotte existante	Écriture	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateScript	Accorde l'autorisation de mettre à jour les métadonnées et le contenu d'un script Serveurs en temps réel existant	Écrire	script*		iam:PassRole s3:GetObject
ValidateMatchmakingRuleSet	Accorde l'autorisation de valider la syntaxe d'un ensemble de règles de FlexMatch matchmaking	Lecture			

Types de ressources définis par les GameLift serveurs Amazon

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
alias	`arn:${Partition}:gamelift:${Region}::alias/${AliasId}`	aws:ResourceTag/${TagKey}
build	`arn:${Partition}:gamelift:${Region}:${Account}:build/${BuildId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
containerGroupDefinition	arn:${Partition}:gamelift:${Region}:${Account}:containergroupdefinition/${Name}	aws:ResourceTag/${TagKey}
containerFleet	arn:${Partition}:gamelift:${Region}:${Account}:containerfleet/${FleetId}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}
gameServerGroup	arn:${Partition}:gamelift:${Region}:${Account}:gameservergroup/${GameServerGroupName}	aws:ResourceTag/${TagKey}
gameSessionQueue	arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}	aws:ResourceTag/${TagKey}
location	arn:${Partition}:gamelift:${Region}:${Account}:location/${LocationId}	aws:ResourceTag/${TagKey}
matchmakingConfiguration	arn:${Partition}:gamelift:${Region}:${Account}:matchmakingconfiguration/${MatchmakingConfigurationName}	aws:ResourceTag/${TagKey}
matchmakingRuleSet	arn:${Partition}:gamelift:${Region}:${Account}:matchmakingruleset/${MatchmakingRuleSetName}	aws:ResourceTag/${TagKey}
script	arn:${Partition}:gamelift:${Region}:${Account}:script/${ScriptId}	aws:ResourceTag/${TagKey}

Clés de condition pour les GameLift serveurs Amazon

Amazon GameLift Servers définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon GameLift Streams

Amazon GameLift Streams (préfixe de service :`gameliftstreams`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon GameLift Streams

- Types de ressources définis par Amazon GameLift Streams
- Clés de condition pour Amazon GameLift Streams

Actions définies par Amazon GameLift Streams

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddStreamGroupLocations	Accorde l'autorisation d'associer un emplacement StreamGroup distant	Écrire	stream group*		ec2:DescribeRegions
AssociateApplications	Accorde l'autorisation d'associer des applications à un StreamGroup	Écrire	application*		
			stream group*		
CreateApplication	Accorde l'autorisation de créer une application	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource s3:GetObject s3:ListBucket

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateStreamGroup	Accorde l'autorisation de créer un StreamGroup	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource
CreateStreamSessionConnection	Accorde l'autorisation de créer une connexion à une session de streaming	Écrire	streamgroup*		
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	application*		
DeleteStreamGroup	Accorde l'autorisation de supprimer un StreamGroup	Écrire	streamgroup*		
DisassociateApplications	Accorde l'autorisation de dissocier les applications d'un StreamGroup	Écrire	application*		
			streamgroup*		
ExportStreamSessionFiles	Accorde l'autorisation d'exporter les fichiers de session de streaming générés par votre application	Écrire	streamgroup*		s3:PutObject
GetApplication	Accorde l'autorisation d'obtenir une application	Lecture	application*		
GetStreamGroup	Accorde la « permission » d'obtenir un StreamGroup	Lecture	streamgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStreamSession	Accorde l'autorisation d'obtenir une session de diffusion	Lecture	stream group*		
ListApplications	Accorde l'autorisation de répertorier les applications	List			
ListStreamGroups	Accorde l'autorisation de mettre en vente StreamGroups	List			
ListStreamSessions	Accorde l'autorisation de répertorier les sessions de streaming	Lecture	stream group*		
ListStreamSessionsByAccount	Accorde l'autorisation de répertorier les sessions de streaming	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture	application		
			stream group		
RemoveStreamGroupLocations	Autorise le détachement d'un site StreamGroup distant	Écrire	stream group*		
StartStreamSession	Accorde l'autorisation de créer une session de diffusion	Écrire	stream group*		
TagResource	Accorde l'autorisation de baliser une ressource	Identification	application		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			stream group		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateStreamSession	Accorde l'autorisation de mettre fin à une session de diffusion	Écrire	stream group*		
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	application		
			stream group		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écrire	application*		
UpdateStreamGroup	Accorde l'autorisation de mettre à jour un StreamGroup	Écrire	stream group*		

Types de ressources définis par Amazon GameLift Streams

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:gameliftstreams:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
stream group	`arn:${Partition}:gameliftstreams:${Region}:${Account}:streamgroup/${StreamGroupId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon GameLift Streams

Amazon GameLift Streams définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS Global Accelerator

AWS Global Accelerator (préfixe de service :`globalaccelerator`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Global Accelerator
- Types de ressources définis par AWS Global Accelerator
- Clés de condition pour AWS Global Accelerator

Actions définies par AWS Global Accelerator

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddCustomRoutingEndpoints	Accorde l'autorisation d'ajouter un point de terminaison de sous-réseau de cloud privé virtuel (VPC) à un groupe de points de terminaison	Écrire	endpointgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	d'accélérateur de routage personnalisé				
AddEndpoints	Accorde l'autorisation d'ajouter un point de terminaison à un groupe de points de terminaison d'accélérateur standard	Écrire	endpointgroup*		globalaccelerator:UpdateEndpointGroup
AdvertiseByoipCidr	Accorde l'autorisation de faire de la publicité pour une plage d' IPv4 adresses destinée à être utilisée avec votre accélérateur via le protocole BYOIP (Bring Your Own IP addresses)	Écrire			
AllowCustomRoutingTraffic	Accorde l'autorisation de permettre le routage personnalisé du trafic utilisateur vers une adresse IP:PORT de destination privée dans un sous-réseau VPC spécifique	Écrire	endpointgroup*		
CreateAccelerator	Accorde l'autorisation de créer un accélérateur standard	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCrossAccountAttachment	Accorde l'autorisation de créer un CrossAccountAttachment	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingAccelerator	Accorde l'autorisation de créer un accélérateur de routage personnalisé	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingEndpointGroup	Accorde l'autorisation de créer un groupe de points de terminaison pour l'écouteur spécifié d'un accélérateur de routage personnalisé	Écrire	listener*		
CreateCustomRoutingListener	Accorde l'autorisation de créer un écouteur pour traiter les connexions entrantes des clients vers un accélérateur de routage personnalisé	Écrire	accelerator*		
CreateEndpointGroup	Accorde l'autorisation d'ajouter un groupe de points de terminaison à un écouteur d'accélérateur standard	Écrire	listener*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateListener	Accorde l'autorisation d'ajouter un écouteur à un accélérateur standard	Écrire	accelerator*		
DeleteAccelerator	Accorde l'autorisation de supprimer un accélérateur standard	Écrire	accelerator*		
DeleteCrossAccountAttachment	Accorde l'autorisation de supprimer un CrossAccountAttachment	Écrire	attachment*		
DeleteCustomRoutingAccelerator	Accorde l'autorisation de supprimer un accélérateur de routage personnalisé	Écrire	accelerator*		
DeleteCustomRoutingEndpointGroup	Accorde l'autorisation de supprimer un groupe de points de terminaison de l'écouteur d'un accélérateur de routage personnalisé	Écrire	endpointgroup*		
DeleteCustomRoutingListener	Accorde l'autorisation de supprimer un écouteur d'un accélérateur de routage personnalisé	Écrire	listener*		
DeleteEndpointGroup	Accorde l'autorisation de supprimer un groupe de points de terminaison associé à un écouteur d'accélérateur standard	Écrire	endpointgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteListener	Accorde l'autorisation de supprimer un écouteur d'un accélérateur standard	Écrire	listener*		
DenyCustomRoutingTraffic	Accorde l'autorisation d'interdire le routage personnalisé du trafic utilisateur vers une adresse IP:PORT de destination privée dans un sous-réseau VPC spécifique	Écrire	endpointgroup*		
DeprovisionByoipCidr	Accorde l'autorisation de libérer la plage d'adresses spécifiée que vous avez configurée pour être utilisée avec votre accélérateur via la solution Fourniture de vos propres adresses IP (BYOIP)	Écrire			
DescribeAccelerator	Accorde l'autorisation de décrire un accélérateur standard	Lecture	accelerator*		
DescribeAcceleratorAttributes	Accorde l'autorisation de décrire les attributs d'un accélérateur standard	Lecture	accelerator*		
DescribeCrossAccountAttachment	Accorde l'autorisation de décrire un CrossAccountAttachment	Lecture	attachment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCustomRoutingAccelerator	Accorde l'autorisation de décrire un accélérateur de routage personnalisé	Lecture	accelerator*		
DescribeCustomRoutingAcceleratorAttributes	Accorde l'autorisation de décrire les attributs d'un accélérateur de routage personnalisé	Lecture	accelerator*		
DescribeCustomRoutingEndpointGroup	Accorde l'autorisation de décrire un groupe de points de terminaison d'un accélérateur de routage personnalisé	Lecture	endpointgroup*		
DescribeCustomRoutingListener	Accorde l'autorisation de décrire un écouteur d'un accélérateur de routage personnalisé	Lecture	listener*		
DescribeEndpointGroup	Accorde l'autorisation de décrire un groupe de points de terminaison d'un accélérateur standard	Lecture	endpointgroup*		
DescribeListener	Accorde l'autorisation de décrire un écouteur d'un accélérateur standard	Lecture	listener*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAccelerators	Accorde l'autorisation de répertorier tous les accélérateurs standard	List			
ListByoipCidrs	Accorde l'autorisation de répertorier les CIDR de vos propres adresses IP (BYOIP)	List			
ListCrossAccountAttachments	Accorde l'autorisation de tout répertorier CrossAccountAttachments	List			
ListCrossAccountResourceAccounts	Accorde l'autorisation de répertorier les comptes CrossAccountAttachments dont l'appelant est indiqué comme principal	List			
ListCrossAccountResources	Accorde l'autorisation de répertorier toutes les CrossAccountAttachment ressources utilisables par l'appelant	List			
ListCustomRoutingAccelerators	Accorde l'autorisation de répertorier les accélérateurs de routage personnalisés pour un Compte AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCustomRoutingEndpointGroups	Accorde l'autorisation de répertorier les groupes de points de terminaison associés à un écouteur d'un accélérateur de routage personnalisé	List	listener*		
ListCustomRoutingListeners	Accorde l'autorisation de répertorier les écouteurs d'un accélérateur de routage personnalisé	List	accelerator*		
ListCustomRoutingPortMappings	Accorde l'autorisation de répertorier les mappages de port d'un accélérateur de routage personnalisé	List	accelerator*		
ListCustomRoutingPortMappingsByDestination	Accorde l'autorisation de répertorier les mappages de port d'une adresse IP de point de terminaison spécifique (une adresse de destination) dans un sous-réseau	List			
ListEndpointGroups	Accorde l'autorisation de répertorier tous les groupes de points de terminaison associés à un écouteur d'accélérateur standard	List	listener*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListListeners	Accorde l'autorisation de répertorier tous les écouteurs associés à un accélérateur standard	List	accelerator*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource globalaccelerator	Lecture	accelerator		
			attachment		
ProvisionByoipCidr	Accorde l'autorisation d'allouer une plage d'adresses pour une utilisation avec votre accélérateur via la solution Fourniture de vos propres adresses IP (BYOIP)	Écrire			
RemoveCustomRoutingEndpoints	Accorde l'autorisation de supprimer un point de terminaison de sous-réseau de cloud privé virtuel (VPC) d'un groupe de points de terminaison d'un accélérateur de routage personnalisé	Écrire	endpointgroup*		
RemoveEndpoints	Accorde l'autorisation de supprimer un point de terminaison d'un groupe de points de terminaison d'accélérateur standard	Écrire	endpointgroup*		globalaccelerator:UpdateEndpointGroup

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter des identifications à une ressource globalaccelerator	Identification	accelerator		
			attachment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource globalaccelerator	Identification	accelerator		
			attachment		
				aws:TagKeys	
UpdateAccelerator	Accorde l'autorisation de mettre à jour un accélérateur standard	Écrire	accelerator*		
UpdateAcceleratorAttributes	Accorde l'autorisation de mettre à jour les attributs d'un accélérateur standard	Écrire	accelerator*		
UpdateCrossAccountAttachment	Accorde l'autorisation de mettre à jour un CrossAccountAttachment	Écrire	attachment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCustomRoutingAccelerator	Accorde l'autorisation de mettre à jour un accélérateur de routage personnalisé	Écrire	accelerator*		
UpdateCustomRoutingAcceleratorAttributes	Accorde l'autorisation de mettre à jour les attributs d'un accélérateur de routage personnalisé	Écrire	accelerator*		
UpdateCustomRoutingListener	Accorde l'autorisation de mettre à jour un écouteur d'un accélérateur de routage personnalisé	Écrire	listener*		
UpdateEndpointGroup	Accorde l'autorisation de mettre à jour un groupe de points de terminaison sur un écouteur d'un accélérateur standard	Écrire	endpointgroup*		
UpdateListener	Accorde l'autorisation de mettre à jour un écouteur sur un accélérateur standard	Écrire	listener*		
WithdrawByoipCidr	Autorise l'arrêt de la publicité pour une adresse BYOIP IPv4	Écrire			

Types de ressources définis par AWS Global Accelerator

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
accelerator	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}`	aws:ResourceTag/${TagKey}
listener	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}`	aws:ResourceTag/${TagKey}
endpointgroup	`arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}/endpoint-group/${EndpointGroupId}`	aws:ResourceTag/${TagKey}
attachment	`arn:${Partition}:globalaccelerator::${Account}:attachment/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Global Accelerator

AWS Global Accelerator définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Glue

AWS Glue (préfixe de service :`glue`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Glue
- Types de ressources définis par AWS Glue
- Clés de condition pour AWS Glue

Actions définies par AWS Glue

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AuthorizeInboundIntegration [autorisation uniquement]	Autorise Glue à valider en permanence que l'ARN cible peut recevoir des données répliquées depuis l'ARN source	Écrire	integration*		
BatchCreatePartition	Accorde l'autorisation de créer une ou plusieurs partitions.	Écriture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
BatchDeleteConnection	Accorde l'autorisation de supprimer une ou plusieurs connexions.	Écriture	connection*		
			rootcatalog*		
				glue:LakeFormationPermissions	
BatchDeletePartition		Écriture	database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de supprimer une ou plusieurs partitions.		rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
BatchDeleteTable	Accorde l'autorisation de supprimer une ou plusieurs tables.	Écriture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
BatchDeleteTableVersion	Accorde l'autorisation de supprimer une ou plusieurs versions d'une table.	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				glue:LakeFormationPermissions	
BatchGetBlueprints	Accorde l'autorisation de récupérer un ou plusieurs plans	Lecture	blueprint*		
BatchGetCrawlers	Accorde l'autorisation de récupérer un ou plusieurs analyseurs.	Lecture	crawler*		
BatchGetCustomEntityTypes	Accorde l'autorisation de récupérer un ou plusieurs types d'entités personnalisées	Lecture			
BatchGetDevEndpoints	Accorde l'autorisation de récupérer un ou plusieurs points de terminaison de développement.	Lecture	devendpoint*		
BatchGetJobs	Accorde l'autorisation de récupérer une ou plusieurs tâches.	Lecture	job*		
BatchGetPartition	Accorde l'autorisation de récupérer une ou plusieurs partitions.	Lecture	database*		
			rootcatalog*		
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			catalog		
				glue:LakeFormationPermissions	
BatchGetStageFiles	Accorde l'autorisation d'obtenir par lots des fichiers de stage pour SparkUI	Gestion des autorisations			
BatchGetTableOptimizer	Accorde l'autorisation de renvoyer la configuration des optimiseurs de table spécifiés.	Lecture	database*		glue:GetTable
			rootcatalog*		
			table*		
BatchGetTriggers	Accorde l'autorisation de récupérer un ou plusieurs déclencheurs.	Lecture	trigger*		
BatchGetWorkflows	Accorde l'autorisation de récupérer un ou plusieurs flux de travail.	Lecture	workflow*		
BatchStopJobRun	Accorde l'autorisation d'arrêter une ou plusieurs exécutions de tâche pour une tâche.	Écrire	job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdatePartition	Accorde l'autorisation de mettre à jour une ou plusieurs partitions	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
CancelDataQualityRuleRecommendationRun	Accorde l'autorisation d'arrêter l'exécution d'une règle de recommandation sur la qualité des données en cours	Écrire	dataQualityRuleset*		
CancelDataQualityRulesetEvaluationRun	Accorde l'autorisation d'arrêter l'exécution d'une évaluation de jeu de règles sur la qualité des données en cours	Écrire	dataQualityRuleset*		
CancelMLTaskRun	Accorde l'autorisation d'arrêter l'exécution d'une tâche de Machine Learning.	Écrire	mlTransform*		
CancelStatement	Accorde l'autorisation d'annuler une déclaration dans une séance interactive	Écrire	session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CheckSchemaVersionValidity	Accorde l'autorisation de récupérer la vérification de la validité de la version d'un schéma	Lecture			
CreateBlueprint	Accorde l'autorisation de créer un plan	Écrire	blueprint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCatalog	Accorde l'autorisation de créer un catalogue	Écrire	catalog*		
			rootcatalog*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
CreateClassifier	Accorde l'autorisation de créer un classifieur.	Écrire			
CreateColumnStatisticsTaskSettings	Accorde l'autorisation de créer des paramètres pour une tâche de statistiques de colonnes	Écrire	database* rootcatalog* table*		
CreateConnection	Accorde l'autorisation de créer une connexion.	Écriture	rootcatalog* connectionType		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys glue:LakeFormationPermissions	
CreateCrawler	Accorde l'autorisation de créer un crawler	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomEntityType	Accorde l'autorisation de créer un type d'entité personnalisée	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityRuleset	Accorde l'autorisation de créer un jeu de règles sur la qualité des données	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDatabase	Accorde l'autorisation de créer une base de données.	Écriture	database*		
			rootcatalog*		
			catalog		
				aws:RequestTag/${TagKey} aws:TagKeys glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
CreateDevEndpoint	Accorde l'autorisation de créer un point de terminaison de développement.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGlueIdentityCenterConfiguration	Accorde l'autorisation de connecter Glue à Identity Center	Écrire			
CreateInboundIntegration [autorisation uniquement]	Autorise le principal source à créer une intégration entrante pour que les données soient répliquées de la source vers la cible	Écrire			
CreateIntegration	Accorde l'autorisation de créer une intégration	Écrire	catalog*		kms:CreateGrant kms:DescribeKey
			connection*		
			database*		
			integration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIntegrationResourceProperty	Accorde l'autorisation de créer une propriété de ressource d'intégration	Écrire	catalog*		
			connection*		
			database*		
			integrationResourceProperty*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationTableProperties	Accorde l'autorisation de créer des propriétés de table d'intégration	Écrire	catalog*		
			connection*		
			database*		
CreateJob	Accorde l'autorisation de créer une tâche.	Écriture	job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateMLTransform	Accorde l'autorisation de créer une transformation ML	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartition	Accorde l'autorisation de créer une partition.	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				glue:LakeFormationPermissions	
CreatePartitionIndex	Accorde l'autorisation de créer un index de partition spécifié dans une table existante	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
CreateRegistry	Accorde l'autorisation de créer un registre de schémas	Écriture	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Accorde l'autorisation de créer un conteneur de schémas	Écriture	registry*		
			schema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	Accorde l'autorisation de créer un script.	Écriture			
CreateSecurityConfiguration	Accorde l'autorisation de créer une configuration de sécurité.	Écrire			
CreateSession	Accorde l'autorisation de créer une séance interactive	Écrire	session*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTable	Accorde l'autorisation de créer une table.	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
CreateTableOptimizer	Accorde l'autorisation de créer un nouvel optimiseur de table pour une fonction spécifique. Le compactage est le seul type d'optimiseur actuellement pris en charge	Écrire	database*		glue:GetTable
			rootcatalog*		
			table*		
CreateTrigger	Accorde l'autorisation de créer un déclencheur.	Écrire	trigger*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageProfile	Accorde l'autorisation de créer un profil d'utilisation	Écrire	usageProfile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserDefinedFunction	Accorde l'autorisation de créer une définition de fonction.	Écriture	database*		
			rootcatalog*		
			catalog		
				glue:LakeFormationPermissions	
CreateWorkflow	Accorde l'autorisation de créer un flux de travail.	Écrire	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBlueprint	Accorde l'autorisation de supprimer un plan	Écrire	blueprint*		
DeleteCatalog	Accorde l'autorisation de supprimer un catalogue	Écrire	rootcatalog*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
DeleteClassifier	Accorde l'autorisation de supprimer un classifieur.	Écrire			
DeleteColumnStatisticsForPartition	Accorde l'autorisation de supprimer les statistiques de colonne de partition d'une colonne	Écrire	database*		
			rootcatalog*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			table*		
			catalog		
				glue:LakeFormationPermissions	
DeleteColumnStatisticsForTable	Accorde l'autorisation de supprimer les statistiques de table des colonnes	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
DeleteColumnStatisticsTaskSettings	Accorde l'autorisation de supprimer les paramètres d'une tâche de statistiques de colonne	Écrire	database*		
			rootcatalog*		
			table*		
DeleteConnection	Accorde l'autorisation de supprimer une connexion.	Écrire	connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			rootcatalog*		
				glue:LakeFormationPermissions	
DeleteConnectionType	Accorde l'autorisation de supprimer le type de connexion	Écrire	connectionType*		
DeleteCrawler	Accorde l'autorisation de supprimer un crawler	Écrire	crawler*		
DeleteCustomEntityType	Accorde l'autorisation de supprimer un type d'entité personnalisée	Écrire			
DeleteDataQualityRuleset	Accorde l'autorisation de supprimer un jeu de règles sur la qualité des données	Écrire	dataQualityRuleset*		
DeleteDatabase	Accorde l'autorisation de supprimer une base de données.	Écriture	database*		
			rootcatalog*		
			table*		
			userdefinedfunction*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
DeleteDevEndpoint	Accorde l'autorisation de supprimer un point de terminaison de développement.	Écrire	devendpoint*		
DeleteGlueIdentityCenterConfiguration	Accorde l'autorisation de déconnecter Glue d'Identity Center	Écrire			
DeleteIntegration	Accorde l'autorisation de supprimer une intégration	Écrire	integration*		
				aws:ResourceTag/${TagKey}	
DeleteIntegrationResourceProperty	Accorde l'autorisation de supprimer la propriété de la ressource d'intégration	Écrire	catalog*		
			connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			database*		
			integrationResourcePropertyArn*		
DeleteIntegrationTableProperties	Autorise la suppression des propriétés de la table d'intégration	Écrire	catalog*		
			connection*		
			database*		
DeleteJob	Accorde l'autorisation de supprimer une tâche.	Écriture	job*		
DeleteMLTransform	Accorde l'autorisation de supprimer une transformation ML	Écriture	mlTransform*		
DeletePartition	Accorde l'autorisation de supprimer une partition.	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				glue:LakeFormationPermissions	
DeletePartitionIndex	Accorde l'autorisation de supprimer un index de partition spécifié d'une table existante	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
DeleteRegistry	Accorde l'autorisation de supprimer un registre de schémas	Écriture	registry*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource.	Gestion des autorisations	rootcatalog*		
DeleteSchema	Accorde l'autorisation de supprimer un conteneur de schémas	Écriture	registry*		
			schema*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSchemaVersions	Accorde l'autorisation de supprimer une plage de versions de schéma	Écriture	registry*		
			schema*		
DeleteSecurityConfiguration	Accorde l'autorisation de supprimer une configuration de sécurité.	Écrire			
DeleteSession	Accorde l'autorisation de supprimer une séance interactive après l'arrêt de la séance si elle n'est pas déjà arrêtée	Écrire	session*		
DeleteTable	Accorde l'autorisation de supprimer une table.	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTableOptimizer	Accorde l'autorisation de supprimer un optimiseur et toutes les métadonnées associées à une table. L'optimisation ne sera plus effectuée sur la table	Écrire	database*		glue:GetTable
			rootcatalog*		
			table*		
DeleteTableVersion	Accorde l'autorisation de supprimer la version d'une table.	Écriture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
DeleteTrigger	Accorde l'autorisation de supprimer un déclencheur.	Écrire	trigger*		
DeleteUsageProfile	Accorde l'autorisation de supprimer un profil d'utilisation	Écrire	usageProfile*		
DeleteUserDefinedFunction	Accorde l'autorisation de supprimer une définition de fonction.	Écriture	database*		
			rootcatalog*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			userdefinedfunction*		
			catalog		
				glue:LakeFormationPermissions	
DeleteWorkflow	Accorde l'autorisation de supprimer un flux de travail.	Écrire	workflow*		
DeregisterDataPreview	Accorde l'autorisation de résilier la session de bloc-notes Glue Studio	Gestion des autorisations			
DescribeConnectionType	Accorde l'autorisation de décrire le type de connexion dans Glue	Gestion des autorisations	connectionType		
DescribeEntity	Donne l'autorisation de décrire une entité dans Glue Studio	Gestion des autorisations	connection*		
			rootcatalog*		
			connectionType		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeInboundIntegrations	Accorde l'autorisation de répertorier les intégrations entrantes	List			
DescribeIntegrations	Accorde l'autorisation de décrire les intégrations Zero-ETL	List	integration*		
				aws:ResourceTag/${TagKey}	
FederateAuthorization	Accorde l'autorisation de lire et d'écrire des ressources fédérées Redshift	Écrire	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery glue:FederatedAuthorizationSource	
GetBlueprint	Accorde l'autorisation de récupérer un plan	Lecture	blueprint*		
GetBlueprintRun	Accorde l'autorisation de récupérer une exécution de plan	Lecture	blueprint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBlueprintRuns	Accorde l'autorisation de récupérer toutes les exécutions d'un plan	Lecture	blueprint*		
GetCatalog	Accorde l'autorisation de récupérer un catalogue	Lecture	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetCatalogImportStatus	Accorde l'autorisation de récupérer le statut d'importation du catalogue.	Lecture	rootcatalog*		
				glue:LakeFormationPermissions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCatalogs	Accorde l'autorisation de récupérer tous les catalogues	Lecture	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetClassifier	Accorde l'autorisation de récupérer un classifieur.	Lecture			
GetClassifiers	Accorde l'autorisation de répertorier tous les classifieurs.	Lecture			
GetColumnStatisticsForPartition	Accorde l'autorisation de récupérer les statistiques de partition des colonnes	Lecture	database*		
			rootcatalog*		
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			catalog		
				glue:LakeFormationPermissions	
GetColumnStatisticsForTable	Accorde l'autorisation de récupérer les statistiques de table des colonnes	Lecture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
GetColumnStatisticsTaskRun	Accorde l'autorisation de récupérer les informations d'exécution des statistiques de colonne pour la table basées sur run-id	Lecture			
GetColumnStatisticsTaskRuns	Accorde l'autorisation de récupérer les informations d'exécution des statistiques de colonne pour la table basées sur run-id	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetColumnStatisticsTaskSettings	Accorde l'autorisation de récupérer les paramètres d'une tâche de statistiques de colonne	Lecture			
GetCompletion	Accorde l'autorisation d'obtenir une réponse générée pour une demande d'achèvement dans Glue from AWS Q	Lecture	completion*		
GetConnection	Accorde l'autorisation de récupérer une connexion.	Lecture	connection*		
			rootcatalog*		
				glue:LakeFormationPermissions	
GetConnections	Accorde l'autorisation de récupérer une liste de connexions.	Lecture	connection*		
			rootcatalog*		
				glue:LakeFormationPermissions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCrawler	Accorde l'autorisation de récupérer un crawler	Lecture	crawler*		
GetCrawlerMetrics	Accorde l'autorisation de récupérer les métriques relatives aux analyseurs.	Lecture			
GetCrawlers	Accorde l'autorisation de récupérer tous les analyseurs.	Lecture			
GetCustomEntityType	Accorde l'autorisation de lire un type d'entité personnalisée	Lecture			
GetDashboardUrl	Accorde l'autorisation de générer une URL présignée pour accéder à l'interface utilisateur de Spark Live	Lecture	session*		
GetDataCatalogEncryptionSettings	Accorde l'autorisation de récupérer les paramètres de chiffrement du catalogue.	Lecture	rootcatalog*		
GetDataPreviewStatement	Octroie l'autorisation d'obtenir une instruction de prévisualisation des données	Gestion des autorisations			
GetDataQualityModel	Autorise la récupération de l'état d'apprentissage du modèle de prédiction pour une statistique	Lecture	dataQualityRuleset*		
			job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataQualityModelResult	Permet de récupérer les prédictions d'une statistique à partir du dernier modèle	Lecture	dataQualityRuleset*		
			job*		
GetDataQualityResult	Accorde l'autorisation de récupérer un résultat sur la qualité des données	Lecture	dataQualityRuleset*		
GetDataQualityRuleRecommendationRun	Accorde l'autorisation de récupérer l'exécution d'une règle de recommandation sur la qualité des données	Lecture	dataQualityRuleset*		
GetDataQualityRuleset	Accorde l'autorisation de récupérer un ensemble de règles sur la qualité des données	Lecture	dataQualityRuleset*		
GetDataQualityRulesetEvaluationRun	Accorde l'autorisation de récupérer l'exécution d'une règle de recommandation sur la qualité des données	Lecture	dataQualityRuleset*		
GetDatabase	Accorde l'autorisation de récupérer une base de données.	Lecture	database*		
			rootcatalog*		
			catalog		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetDatabases	Accorde l'autorisation de récupérer toutes les bases de données.	Lecture	database*		
			rootcatalog*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetDataflowGraph	Accorde l'autorisation de transformer un script en graphe orienté acyclique (DAG).	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDevEndpoint	Accorde l'autorisation de récupérer un point de terminaison de développement.	Lecture	devendpoint*		
GetDevEndpoints	Accorde l'autorisation de récupérer tous les points de terminaison de développement.	Lecture			
GetEntityRecords	Accorde l'autorisation de prévisualiser les enregistrements d'entités dans Glue	Lecture	catalog*		
			connection		
			connectionType		
GetEnvironment	Accorde l'autorisation d'obtenir les détails de l'environnement pour SparkUI	Gestion des autorisations			
GetExecutors	Accorde l'autorisation d'obtenir des exécuteurs pour SparkUI	Gestion des autorisations			
GetExecutorsThreads	Accorde l'autorisation d'obtenir des threads d'exécution pour SparkUI	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGeneratedCode	Transforme un graphe acyclique dirigé (DAG) en code	Lecture			
GetGlueIdentityCenterConfiguration	Accorde l'autorisation de récupérer l'application Idc gérée	Lecture			
GetIntegrationResourceProperty	Accorde l'autorisation de récupérer la propriété de la ressource d'intégration	Lecture	catalog*		
			connection*		
			database*		
			integrationResourceProperty*		
GetIntegrationTableProperties	Accorde l'autorisation de récupérer les propriétés de la table d'intégration	Lecture	catalog*		
			connection*		
			database*		
GetJob	Accorde l'autorisation de récupérer une tâche.	Lecture	job*		
GetJobBookmark	Accorde l'autorisation de récupérer un signet de tâche.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetJobRun	Accorde l'autorisation de récupérer une exécution de tâche.	Lecture	job*		
GetJobRuns	Accorde l'autorisation de récupérer toutes les exécutions de tâche d'une tâche.	Lecture	job*		
GetJobUpgradeAnalysis	Accorde l'autorisation de récupérer une analyse de mise à niveau pour une tâche	Lecture	job*		
GetJobs	Accorde l'autorisation de récupérer toutes les tâches en cours.	Lecture			
GetLogParsingStatus	Accorde l'autorisation d'obtenir le statut d'analyse du journal pour SparkUI	Gestion des autorisations			
GetMLTaskRun	Accorde l'autorisation de récupérer une exécution de tâche ML	Lecture	mlTransform*		
GetMLTaskRuns	Accorde l'autorisation de récupérer toutes les exécutions de tâche ML	Liste	mlTransform*		
GetMLTransform	Accorde l'autorisation de récupérer une transformation ML	Lecture	mlTransform*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMLTransforms	Accorde l'autorisation de récupérer toutes les transformations ML	Liste	mlTransform*		
GetMapping	Accorde l'autorisation de créer un mappage.	Lecture			
GetNotebookInstanceStatus	Accorde l'autorisation de récupérer l'état de session de blocs-notes Glue Studio	Gestion des autorisations			
GetPartition	Accorde l'autorisation de récupérer une partition.	Lecture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
GetPartitionIndexes	Accorde l'autorisation de récupérer les index de partition pour une table	Lecture	database*		
			rootcatalog*		
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			catalog		
				glue:LakeFormationPermissions	
GetPartitions	Accorde l'autorisation de récupérer les partitions d'une table.	Lecture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
GetPlan	Accorde l'autorisation de récupérer un mappage pour un script.	Lecture			
GetQueries	Accorde l'autorisation d'obtenir des requêtes pour SparkUI	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQuery	Accorde l'autorisation d'obtenir une requête spécifique pour SparkUI	Gestion des autorisations			
GetRecipeAction	Accorde l'autorisation d'obtenir le résultat d'une déclaration de recette de préparation des données	Gestion des autorisations			
GetRegistry	Accorde l'autorisation de récupérer un registre de schémas	Lecture	registry*		
GetResourcePolicies	Accorde l'autorisation de récupérer les stratégies de ressource	Lecture	rootcatalog*		
GetResourcePolicy	Accorde l'autorisation de récupérer une politique de ressource.	Lecture	rootcatalog*		
GetSchema	Accorde l'autorisation de récupérer un conteneur de schémas	Lecture	registry* schema*		
GetSchemaByDefinition	Accorde l'autorisation de récupérer une version de schéma en fonction de la définition du schéma	Lecture	registry* schema*		
GetSchemaVersion		Lecture	registry		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de récupérer une version de schéma		schema		
GetSchemaVersionsDiff	Accorde l'autorisation de comparer deux versions de schéma dans le registre des schémas	Lecture	registry* schema*		
GetSecurityConfiguration	Accorde l'autorisation de récupérer une configuration de sécurité.	Lecture			
GetSecurityConfigurations	Accorde l'autorisation de récupérer une ou plusieurs configurations de sécurité.	Lecture			
GetSession	Accorde l'autorisation de récupérer une séance interactive	Lecture	session*		
GetStage	Donne l'autorisation d'obtenir un stage pour SparkUI	Gestion des autorisations			
GetStageAttempt	Accorde l'autorisation d'effectuer une tentative de stage pour SparkUI	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStageAttemptTaskList	Accorde l'autorisation d'obtenir la liste des tâches pour une tentative d'étape pour SparkUI	Gestion des autorisations			
GetStageAttemptTaskSummary	Accorde l'autorisation d'obtenir le résumé de la tâche pour une tentative d'étape pour SparkUI	Gestion des autorisations			
GetStageFiles	Accorde l'autorisation d'obtenir des fichiers de scène pour SparkUI	Gestion des autorisations			
GetStages	Donne l'autorisation d'obtenir des stages pour SparkUI	Gestion des autorisations			
GetStatement	Accorde l'autorisation de récupérer des résultats et des informations sur une déclaration dans une séance interactive	Lecture	session*		
GetStorage	Accorde l'autorisation d'obtenir les détails de stockage pour SparkUI	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStorageUnit	Accorde l'autorisation d'obtenir les détails de l'unité de stockage pour SparkUI	Gestion des autorisations			
GetTable	Accorde l'autorisation de récupérer une table.	Lecture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetTableOptimizer	Accorde l'autorisation de renvoyer la configuration de tous les optimiseurs associés à une table spécifiée	Lecture	database*		glue:GetTable
			rootcatalog*		
			table*		
GetTableVersion		Lecture	database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de récupérer une version d'une table.		rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
GetTableVersions	Accorde l'autorisation de récupérer une liste des versions d'une table.	Lecture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
GetTables	Accorde l'autorisation de récupérer les tables dans une base de données.	Lecture	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetTags	Accorde l'autorisation de récupérer toutes les balises associées à une ressource.	Lecture	blueprint		
			catalog		
			connection		
			connectionType		
			crawler		
			customEntityType		
			database		
			devendpoint		
			job		
			trigger		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			usageProfile		
			workflow		
GetTrigger	Accorde l'autorisation de récupérer un déclencheur.	Lecture	trigger*		
GetTriggers	Accorde l'autorisation de récupérer les déclencheurs associés à une tâche.	Lecture			
GetUsageProfile	Accorde l'autorisation de récupérer un profil d'utilisation	Lecture	usageProfile*		
GetUserDefinedFunction	Accorde l'autorisation de récupérer une définition de fonction	Lecture	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
				glue:LakeFormationPermissions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetUserDefinedFunctions	Accorde l'autorisation de récupérer plusieurs définitions de fonction.	Lecture	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetWorkflow	Accorde l'autorisation de récupérer un flux de travail.	Lecture	workflow*		
GetWorkflowRun	Accorde l'autorisation de récupérer une exécution de flux de travail	Lecture	workflow*		
GetWorkflowRunProperties	Accorde l'autorisation de récupérer les propriétés d'exécution de flux de travail	Lecture	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkflowRuns	Accorde l'autorisation de récupérer toutes les exécutions d'un flux de travail.	Lecture	workflow*		
GlueNotebookAuthorize	Accorde l'autorisation d'accéder aux blocs-notes Glue Studio	Gestion des autorisations			
GlueNotebookRefreshCredentials	Accorde l'autorisation d'actualiser les informations d'identification des blocs-notes Glue Studio	Gestion des autorisations			
ImportCatalogToGlue	Autorise l'importation d'un catalogue de données Athena dans Glue AWS	Écrire	rootcatalog*		
				glue:LakeFormationPermissions	
ListBlueprints	Accorde l'autorisation de récupérer tous les plans	List			
ListColumnStatisticsTaskRuns	Accorde l'autorisation de répertorier tous les identifiants d'exécution des statistiques de colonne qui ont été exécutés pour le compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConnectionTypes	Accorde l'autorisation de répertorier les types de connexion dans Glue	Gestion des autorisations			
ListCrawlers	Accorde l'autorisation de récupérer tous les analyseurs.	List			
ListCrawls	Accorde l'autorisation de récupérer l'historique des cycles de crawler pour un crawl	List	crawler*		
ListCustomEntityTypes	Accorde l'autorisation de récupérer tous les types d'entités personnalisées	List			
ListDataQualityResults	Accorde l'autorisation de récupérer tous les résultats sur la qualité des données	List	dataQualityRuleset*		
ListDataQualityRuleRecommendationRuns	Accorde l'autorisation de récupérer les exécutions de règle de recommandation sur la qualité des données	List	dataQualityRuleset*		
ListDataQualityRulesetEvaluationRuns	Accorde l'autorisation de récupérer les exécutions de règle de recommandation sur la qualité des données	List	dataQualityRuleset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDataQualityRulesets	Accorde l'autorisation de récupérer une liste des ensembles de règles sur la qualité des données	List	dataQualityRuleset*		
ListDevEndpoints	Accorde l'autorisation de récupérer tous les points de terminaison de développement.	List			
ListEntities	Accorde l'autorisation de répertorier des entités dans Glue Studio	Gestion des autorisations	connection*		
			rootcatalog*		
			connectionType		
ListIntegrationResourceProperties	Accorde l'autorisation de répertorier les propriétés des ressources d'intégration Zero-ETL	List	catalog*		
			connection*		
			database*		
			integrationResourcceProperty*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListJobUpgradeAnalyses	Permet de répertorier les analyses de mise à niveau pour une tâche	List	job*		
ListJobs	Accorde l'autorisation de récupérer toutes les tâches en cours.	Liste			
ListMLTransforms	Accorde l'autorisation de récupérer toutes les transformations ML	Liste	mlTransform*		
ListRegistries	Accorde l'autorisation de récupérer une liste de registres de schémas	Liste			
ListSchemaVersions	Accorde l'autorisation de récupérer une liste de versions de schéma	Liste	registry*		
			schema*		
ListSchemas	Accorde l'autorisation de récupérer une liste de conteneurs de schémas	List	registry		
ListSessions	Accorde l'autorisation de récupérer une liste de séances interactives	List			
ListStatements	Accorde l'autorisation de récupérer une liste des déclarations d'une séance interactive	List	session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTableOptimizerRuns	Accorde l'autorisation de répertorier l'historique des exécutions précédentes de l'optimiseur pour une table spécifique	List	database*		glue:GetTable
			rootcatalog*		
			table*		
ListTriggers	Accorde l'autorisation de récupérer tous les déclencheurs.	List			
ListUsageProfiles	Accorde l'autorisation de récupérer une liste de profils d'utilisation	List			
ListWorkflows	Accorde l'autorisation de récupérer tous les flux de travail.	List			
ModifyIntegration	Accorde l'autorisation de modifier une intégration Zero-ETL	Écrire	integration*		
				aws:ResourceTag/${TagKey}	
NotifyEvent	Autorise l'autorisation de notifier un événement au flux de travail basé sur les événements	Écrire	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PassConnection [autorisation uniquement]	Accorde l'autorisation de transmettre le nom de la connexion glue en entrée pour ceux APIs qui en ont besoin	Écrire	connection*		
PublishDataQuality [autorisation uniquement]	Accorde l'autorisation de publier des résultats sur la qualité des données	Écrire	dataQualityRuleset*		
PutDataCatalogEncryptionSettings	Accorde l'autorisation de mettre à jour les paramètres de chiffrement du catalogue.	Écrire	rootcatalog*		
PutDataQualityProfileAnnotation	Accorde l'autorisation d'annoter tous les points de données d'un profil	Écrire	dataQualityRuleset*		
			job*		
PutDataQualityStatisticAnnotation	Accorde l'autorisation d'annoter des points de données au fil du temps pour une statistique de qualité des données spécifique	Écrire	dataQualityRuleset*		
			job*		
PutResourcePolicy	Accorde l'autorisation de mettre à jour une politique de ressource.	Gestion des autorisations	rootcatalog*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutSchemaVersionMetadata	Accorde l'autorisation d'ajouter des métadonnées à une version de schéma	Écriture	registry		
			schema		
PutWorkflowRunProperties	Accorde l'autorisation de mettre à jour les propriétés d'exécution de flux de travail	Écriture	workflow*		
QuerySchemaVersionMetadata	Accorde l'autorisation de récupérer les métadonnées d'une version de schéma	List	registry		
			schema		
RefreshOAuth2Tokens	Accorde l'autorisation d'actualiser les jetons oauth2 pour la connexion pendant l'exécution de la tâche	Gestion des autorisations	connection*		
			rootcatalog*		
			connectionType		
RegisterConnectionType	Accorde l'autorisation d'enregistrer le type de connexion	Écrire	connectionType*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RegisterSchemaVersion	Accorde l'autorisation de créer une version de schéma	Écriture	registry*		
			schema*		
RemoveSchemaVersionMetadata	Accorde l'autorisation de supprimer les métadonnées d'une version de schéma	Écrire	registry		
			schema		
RenameTable	Accorde l'autorisation de renommer une table	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
RequestLogParsing	Accorde l'autorisation de demander l'analyse du journal pour SparkUI	Gestion des autorisations			
ResetJobBookmark	Accorde l'autorisation de réinitialiser un signet de tâche.	Écriture			
ResumeWorkflowRun	Accorde l'autorisation de reprendre l'exécution d'un flux de travail	Écrire	workflow*		
RunDataPreviewStatement	Octroie l'autorisation d'exécuter une instruction de prévisualisation des données	Gestion des autorisations			
RunStatement	Accorde l'autorisation d'exécuter un code ou une déclaration dans une séance interactive	Écrire	session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchTables	Accorde l'autorisation de récupérer les tables du catalogue.	Lecture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
SendFeedback	Accorde l'autorisation de fournir des commentaires sur une expérience de réalisation de colle dans AWS Q	Écrire			
SendRecipeAction	Autorise l'exécution d'une instruction Data Preparation Recipe dans l'aperçu des données	Gestion des autorisations			
StartBlueprintRun	Accorde l'autorisation de démarrer l'exécution d'un plan	Écrire	blueprint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartColumnStatisticsTaskRun	Accorde l'autorisation de démarrer une exécution pour générer des statistiques de colonne pour la table	Écrire	database*		glue:GetSecurityConfiguration glue:GetTable
			rootcatalog*		
			table*		
StartColumnStatisticsTaskRunSchedule	Accorde l'autorisation de démarrer le calendrier d'exécution d'une tâche de statistiques de colonne	Écrire	database*		
			rootcatalog*		
			table*		
StartCompletion	Accorde l'autorisation de créer une demande d'achèvement dans l'expérience Glue for AWS Q	Écrire			
StartCrawler	Accorde l'autorisation de démarrer un crawler	Écriture	crawler*		
StartCrawlerSchedule	Accorde l'autorisation de modifier l'état de la planification d'un crawler sur SCHEDULED	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDataQualityRuleRecommendationRun	Accorde l'autorisation de démarrer l'exécution d'une règle de recommandation sur la qualité des données	Écrire	dataQualityRuleset*		
StartDataQualityRulesetEvaluationRun	Accorde l'autorisation de démarrer l'exécution d'une règle de recommandation sur la qualité des données	Écrire	dataQualityRuleset*		
StartExportLabelsTaskRun	Accorde l'autorisation de démarrer l'exécution d'une tâche du Machine Learning d'exportation des étiquettes	Écriture	mlTransform*		
StartImportLabelsTaskRun	Accorde l'autorisation de démarrer l'exécution d'une tâche du Machine Learning d'importation des étiquettes	Écriture	mlTransform*		
StartJobRun	Accorde l'autorisation de lancer l'exécution d'une tâche.	Écrire	job*		
StartJobUpgradeAnalysis	Autorise le lancement d'une analyse de mise à niveau pour une tâche	Écrire	job*		
StartMLEvaluationTaskRun	Accorde l'autorisation de démarrer l'exécution d'une tâche du Machine Learning d'évaluation	Écriture	mlTransform*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMLLabelingSetGenerationTaskRun	Accorde l'autorisation de démarrer l'exécution d'une tâche du Machine Learning d'étiquetage de la génération des ensembles	Écrire	mlTransform*		
StartNotebook	Accorde l'autorisation de lancer des blocs-notes Glue Studio	Gestion des autorisations			
StartTrigger	Accorde l'autorisation de démarrer un déclencheur.	Écriture	trigger*		
StartWorkflowRun	Accorde l'autorisation de lancer l'exécution d'un flux de travail.	Écrire	workflow*		
StopColumnStatisticsTaskRun	Accorde l'autorisation d'arrêter l'exécution des statistiques de colonne	Écrire	database*		
			rootcatalog*		
			table*		
StopColumnStatisticsTaskRunSchedule	Autorise l'arrêt du calendrier d'exécution d'une tâche de statistiques de colonne	Écrire	database*		
			rootcatalog*		
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopCrawler	Accorde l'autorisation d'arrêter un crawler en cours d'exécution.	Écriture	crawler*		
StopCrawlerSchedule	Accorde l'autorisation de définir l'état de la planification d'un crawler sur NOT_SCHEDULED	Écrire			
StopJobUpgradeAnalysis	Autorise l'arrêt d'une analyse de mise à niveau en cours pour une tâche	Écrire	job*		
StopSession	Accorde l'autorisation d'arrêter une séance interactive	Écrire	session*		
StopTrigger	Accorde l'autorisation d'arrêter un déclencheur.	Écriture	trigger*		
StopWorkflowRun	Accorde l'autorisation d'arrêter l'exécution d'un flux de travail	Écriture	workflow*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Identification	blueprint		
			catalog		
			connection		
			connectionType		
			crawler		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			customEntityType		
			dataQualityRuleset		
			database		
			devendpoint		
			integration		
			integrationResourceProperty		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey} glue:LakeFormationPermissions	
TerminateNotebook	Accorde l'autorisation de résilier des blocs-notes Glue Studio	Gestion des autorisations			
TestConnection	Accorde l'autorisation de tester la connexion dans Glue Studio.	Gestion des autorisations	connection		
			connectionType		
UntagResource	Accorde l'autorisation de supprimer les balises associées à une ressource.	Identification	blueprint		
			catalog		
			connection		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			connectionType		
			crawler		
			customEntityType		
			dataQualityRuleset		
			database		
			devendpoint		
			integration		
			integrationResourceProperty		
			job		
			mlTransform		
			registry		
			schema		
			session		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys glue:LakeFormationPermissions	
UpdateBlueprint	Accorde l'autorisation de mettre à jour un plan	Écrire	blueprint*		
UpdateCatalog	Accorde l'autorisation de mettre à jour un catalogue	Écrire	rootcatalog*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateClassifier	Accorde l'autorisation de mettre à jour un classifieur.	Écrire			
UpdateColumnStatisticsForPartition	Accorde l'autorisation de mettre à jour les statistiques de partition des colonnes	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
UpdateColumnStatisticsForTable	Accorde l'autorisation de mettre à jour les statistiques de table des colonnes	Écrire	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateColumnStatisticsTaskSettings	Accorde l'autorisation de mettre à jour les paramètres d'une tâche de statistiques de colonne	Écrire	database*		
			rootcatalog*		
			table*		
UpdateConnection	Accorde l'autorisation de mettre à jour une connexion.	Écriture	connection*		
			rootcatalog*		
			connectionType		
				glue:LakeFormationPermissions	
UpdateCrawler	Accorde l'autorisation de mettre à jour un crawler	Écriture	crawler*		
UpdateCrawlerSchedule	Accorde l'autorisation de mettre à jour la planification d'un crawler	Écrire			
UpdateDataQualityRuleset	Accorde l'autorisation de mettre à jour un ensemble de règles sur la qualité des données	Écrire	dataQualityRuleset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDatabase	Accorde l'autorisation de mettre à jour une base de données.	Écriture	database*		
			rootcatalog*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
UpdateDevEndpoint	Accorde l'autorisation de mettre à jour un point de terminaison de développement.	Écrire	devendpoint*		
UpdateGlueIdentityCenterConfiguration	Accorde l'autorisation de mettre à jour l'application Idc gérée	Écrire			
UpdateIntegrationResourceProperty	Accorde l'autorisation de mettre à jour la propriété de la ressource d'intégration	Écrire	catalog*		
			connection*		
			database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			integrationResourceProperty*		
UpdateIntegrationTablePropertes	Autorise la mise à jour des propriétés de la table d'intégration	Écrire	catalog*		
			connection*		
			database*		
UpdateJob	Accorde l'autorisation de mettre à jour une tâche.	Écrire	job*		
				glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
UpdateJobFromSourceControl	Accorde l'autorisation de mettre à jour une tâche à partir du fournisseur de contrôle de source	Écrire	job*		
UpdateMLTransform	Accorde l'autorisation de mettre à jour une transformation ML	Écriture	mlTransform*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePartition	Accorde l'autorisation de mettre à jour une partition.	Écriture	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
UpdateRegistry	Accorde l'autorisation de mettre à jour un registre de schémas	Écriture	registry*		
UpdateSchema	Accorde l'autorisation de mettre à jour un conteneur de schémas	Écrire	registry*		
			schema*		
UpdateSourceControlFromJob	Accorde l'autorisation de mettre à jour le fournisseur de contrôle de source à partir d'une tâche	Écrire	job*		
UpdateTable	Accorde l'autorisation de mettre à jour une table.	Écrire	database*		
			rootcatalog*		
			table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
UpdateTableOptimizer	Accorde l'autorisation de mette à jour la configuration d'un optimiseur de table existant	Écrire	database*		glue:GetTable
			rootcatalog*		
			table*		
UpdateTrigger	Accorde l'autorisation de mettre à jour un déclencheur.	Écrire	trigger*		
UpdateUsageProfile	Accorde l'autorisation de mettre à jour un profil d'utilisation	Écrire	usageProfile*		
UpdateUserDefinedFunction	Accorde l'autorisation de mettre à jour une définition de fonction.	Écriture	database*		
			rootcatalog*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			userdefinedfunction*		
			catalog		
				glue:LakeFormationPermissions	
UpdateWorkflow	Accorde l'autorisation de mettre à jour un flux de travail.	Écrire	workflow*		
UpgradeJob	Autorise la mise à niveau d'une tâche vers la dernière version	Écrire	job*		
UseGlueStudio	Accorde l'autorisation d'utiliser Glue Studio et d'accéder à son site interne APIs	Gestion des autorisations			
UseMLTransforms [autorisation uniquement]	Accorde l'autorisation d'utiliser une transformation ML à partir d'un script ETL Glue	Écrire	mlTransform*		

Types de ressources définis par AWS Glue

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
rootcatalog	`arn:${Partition}:glue:${Region}:${Account}:catalog`	
catalog	`arn:${Partition}:glue:${Region}:${Account}:catalog/${CatalogName}`	aws:ResourceTag/${TagKey}
database	`arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:glue:${Region}:${Account}:table/${DatabaseName}/${TableName}`	
tableversion	`arn:${Partition}:glue:${Region}:${Account}:tableVersion/${DatabaseName}/${TableName}/${TableVersionName}`	
connection	`arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}`	aws:ResourceTag/${TagKey}
userdefinedfunction	`arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${DatabaseName}/${UserDefinedFunctionName}`	
devendpoint	`arn:${Partition}:glue:${Region}:${Account}:devEndpoint/${DevEndpointName}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:glue:${Region}:${Account}:job/${JobName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
trigger	arn:${Partition}:glue:${Region}:${Account}:trigger/${TriggerName}	aws:ResourceTag/${TagKey}
crawler	arn:${Partition}:glue:${Region}:${Account}:crawler/${CrawlerName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:glue:${Region}:${Account}:workflow/${WorkflowName}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:glue:${Region}:${Account}:blueprint/${BlueprintName}	aws:ResourceTag/${TagKey}
mlTransform	arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}	aws:ResourceTag/${TagKey}
registry	arn:${Partition}:glue:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}
schema	arn:${Partition}:glue:${Region}:${Account}:schema/${SchemaName}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:glue:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
usageProfile	arn:${Partition}:glue:${Region}:${Account}:usageProfile/${UsageProfileId}	aws:ResourceTag/${TagKey}
dataQualityRuleset	arn:${Partition}:glue:${Region}:${Account}:dataQualityRuleset/${RulesetName}	aws:ResourceTag/${TagKey}
customEntityType	arn:${Partition}:glue:${Region}:${Account}:customEntityType/${CustomEntityTypeId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
completion	arn:${Partition}:glue:${Region}:${Account}:completion/${CompletionId}	
integration	arn:${Partition}:glue:${Region}:${Account}:integration:${IntegrationId}	aws:ResourceTag/${TagKey}
connectionType	arn:${Partition}:glue:${Region}:${Account}:connectionType:${ConnectionTypeName}	aws:ResourceTag/${TagKey}
integrationResourceProperty	arn:${Partition}:glue:${Region}:${Account}:integrationresourceproperty/${ResourceType}/${ResourceName}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Glue

AWS Glue définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Clés de condition	Description	Type
glue:CredentialIssuingService	Filtre l'accès par le service à l'aide duquel les informations d'identification de la demande sont émises	String
glue:EnabledForRedshiftAutoDiscovery	Filtre l'accès en fonction de la présence de la clé configurée pour la politique basée sur l'identité du rôle	Booléen
glue:FederatedAuthorizationSource	Filtre l'accès en fonction de l'appartenance de la ressource à une autorisation fédérée	String
glue:LakeFormationPermissions	Filtre l'accès selon que les vérifications d'autorisation de Lake Formation seront effectuées pour un appelant donné et pour la ressource Glue	String
glue:RoleAssumedBy	Filtre l'accès par le service à l'aide duquel les informations d'identification de la demande sont obtenues en endossant le rôle de client	String
glue:SecurityGroupIds	Filtre l'accès en fonction de l'ID des groupes de sécurité configurés pour la tâche Glue	ArrayOfString
glue:SubnetIds	Filtre l'accès en fonction de l'ID des sous-réseaux configurés pour la tâche Glue	ArrayOfString
glue:VpcIds	Filtre l'accès en fonction de l'ID du VPC configuré pour la tâche Glue	ArrayOfString

Actions, ressources et clés de condition pour AWS Glue DataBrew

AWS Glue DataBrew (préfixe de service :`databrew`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Glue DataBrew
- Types de ressources définis par AWS Glue DataBrew
- Clés de condition pour AWS Glue DataBrew

Actions définies par AWS Glue DataBrew

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDeleteRecipeVersion	Accorde l'autorisation de supprimer une ou plusieurs versions de recette	Écriture	Recipe*		
CreateDataset	Accorde l'autorisation de créer un jeu de données.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CreateProfileJob	Accorde l'autorisation de créer une tâche de profil	Écriture		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProject	Accorde l'autorisation de créer un projet	Écriture		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRecipe	Accorde l'autorisation de créer une recette	Écriture		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecipeJob	Accorde l'autorisation de créer une tâche de recette	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRuleset	Accorde l'autorisation de créer un ensemble de règles	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSchedule	Accorde l'autorisation de créer une planification	Écriture		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données.	Écriture	Dataset*		
DeleteJob	Accorde l'autorisation de supprimer une tâche.	Écriture	Job*		
DeleteProject	Accorde l'autorisation de supprimer un projet	Écriture	Project*		
DeleteRecipeVersion	Accorde l'autorisation de supprimer une version de recette	Écrire	Recipe*		
DeleteRuleset	Accorde l'autorisation de supprimer un ensemble de règles	Écrire	Ruleset*		
DeleteSchedule	Accorde l'autorisation de supprimer une planification	Écriture	Schedule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDataset	Accorde l'autorisation d'afficher les informations sur un jeu de données	Lecture	Dataset*		
DescribeJob	Accorde l'autorisation d'afficher les informations sur une tâche	Lecture	Job*		
DescribeJobRun	Accorde l'autorisation d'afficher les détails sur l'exécution de tâche d'une tâche donnée	Lecture	Job*		
DescribeProject	Accorde l'autorisation d'afficher les informations sur un projet	Lecture	Project*		
DescribeRecipe	Accorde l'autorisation d'afficher les informations sur une recette	Lecture	Recipe*		
DescribeRuleset	Accorde l'autorisation d'afficher les informations sur un ensemble de règles	Lecture	Ruleset*		
DescribeSchedule	Accorde l'autorisation d'afficher les informations sur une planification	Lecture	Schedule*		
ListDatasets	Accorde l'autorisation de répertorier les jeux de données de votre compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListJobRuns	Accorde l'autorisation de répertorier les exécutions de tâche d'une tâche donnée	Lecture	Job*		
ListJobs	Accorde l'autorisation de répertorier les tâches de votre compte	Lecture			
ListProjects	Accorde l'autorisation de répertorier les projets de votre compte	Lecture			
ListRecipeVersions	Accorde l'autorisation de répertorier les versions de votre recette	Lecture	Recipe*		
ListRecipes	Accorde l'autorisation de répertorier les recettes de votre compte	Lecture			
ListRulesets	Accorde l'autorisation de répertorier les ensembles de règles de votre compte	Lecture			
ListSchedules	Accorde l'autorisation de répertorier les planifications de votre compte	Lecture			
ListTagsForResource	Accorde l'autorisation de récupérer les balises associées à une ressource	Lecture	Dataset		
			Job		
			Project		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Recipe		
			Ruleset		
			Schedule		
PublishRecipe	Accorde l'autorisation de publier une version majeure d'une recette	Écriture	Recipe*		
SendProjectSessionAction	Accorde l'autorisation de soumettre une action à la séance interactive d'un projet	Écriture	Project*		
StartJobRun	Accorde l'autorisation de lancer l'exécution d'une tâche.	Écriture	Job*		
StartProjectSession	Accorde l'autorisation de démarrer une séance interactive d'un projet	Écriture	Project*		
StopJobRun	Accorde l'autorisation d'arrêter l'exécution d'une tâche	Écriture	Job*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Schedule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises associées à une ressource.	Balisage	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:TagKeys	
UpdateDataset	Accorde l'autorisation de modifier un jeu de données	Écriture	Dataset*		
UpdateProfileJob	Accorde l'autorisation de modifier une tâche de profil	Écriture	Job*		
UpdateProject	Accorde l'autorisation de modifier un projet	Écriture	Project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRecipe	Accorde l'autorisation de modifier une recette	Écriture	Recipe*		
UpdateRecipeJob	Accorde l'autorisation de modifier une tâche de recette	Écrire	Job*		
UpdateRuleset	Accorde l'autorisation de modifier un ensemble de règles	Écrire	Ruleset*		
UpdateSchedule	Accorde l'autorisation de modifier une planification	Écrire	Schedule*		

Types de ressources définis par AWS Glue DataBrew

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Project	`arn:${Partition}:databrew:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}
Dataset	`arn:${Partition}:databrew:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Ruleset	arn:${Partition}:databrew:${Region}:${Account}:ruleset/${ResourceId}	aws:ResourceTag/${TagKey}
Recipe	arn:${Partition}:databrew:${Region}:${Account}:recipe/${ResourceId}	aws:ResourceTag/${TagKey}
Job	arn:${Partition}:databrew:${Region}:${Account}:job/${ResourceId}	aws:ResourceTag/${TagKey}
Schedule	arn:${Partition}:databrew:${Region}:${Account}:schedule/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Glue DataBrew

AWS Glue DataBrew définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Ground Station

AWS Ground Station (préfixe de service :`groundstation`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Ground Station
- Types de ressources définis par AWS Ground Station
- Clés de condition pour AWS Ground Station

Actions définies par AWS Ground Station

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelContact	Accorde l'autorisation d'annuler un contact.	Écriture	Contact*		
CreateConfig	Accorde l'autorisation de créer une configuration.	Écriture		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateDataflowEndpointGroup	Accorde l'autorisation de créer un groupe de points de terminaison de flux de données.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataflowEndpointGroupV2	Accorde l'autorisation de créer un groupe de points de terminaison de flux de données à l'aide de l'opération V2	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEphemeris	Accorde l'autorisation de créer un modèle d'e-mail	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMissionProfile	Accorde l'autorisation de créer un profil de mission.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfig	Accorde l'autorisation de supprimer une configuration.	Écriture	Config*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDataflowEndpointGroup	Accorde l'autorisation de supprimer un groupe de points de terminaison de flux de données.	Écrire	DataflowEndpointGroup*		
DeleteEphemeris	Accorde l'autorisation de supprimer un modèle d'e-mail	Écrire	EphemerisItem*		
DeleteMissionProfile	Accorde l'autorisation de supprimer un profil de mission.	Écriture	MissionProfile*		
DescribeContact	Accorde l'autorisation de décrire un contact.	Lecture	Contact*		
DescribeEphemeris	Autorise la description d'un élément d'autorisation	Lecture	EphemerisItem*		
GetAgentConfiguration	Octroie l'autorisation d'obtenir la configuration d'un agent	Lecture	Agent*		
GetAgentTaskResponseUrl	Accorde l'autorisation de récupérer la journalisation S3 présignée URLs	Lecture	Agent*		
GetConfig	Accorde l'autorisation de renvoyer une configuration.	Lecture	Config*		
GetDataflowEndpointGroup	Accorde l'autorisation de renvoyer un groupe de points de terminaison de flux de données.	Lecture	DataflowEndpointGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMinuteUsage	Accorde l'autorisation de renvoyer l'utilisation en minutes.	Lecture			
GetMissionProfile	Accorde l'autorisation de récupérer un profil de mission.	Lecture	MissionProfile*		
GetSatellite	Accorde l'autorisation de renvoyer des informations sur un satellite.	Lecture	Satellite*		
ListConfigs	Accorde l'autorisation de renvoyer une liste des anciennes configurations.	Liste			
ListContacts	Accorde l'autorisation de renvoyer une liste des contacts.	Liste			
ListDataflowEndpointGroups	Accorde l'autorisation de répertorier les groupes de points de terminaison de flux de données.	List			
ListEphemerides	Accorde l'autorisation de répertorier tous les périphériques	List			
ListGroundStations	Accorde l'autorisation de répertorier les stations au sol.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMissionProfiles	Accorde l'autorisation de renvoyer une liste des profils de mission.	Liste			
ListSatellites	Accorde l'autorisation de répertorier les satellites.	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	Config		
			Contact		
			DataflowEndpointGroup		
			MissionProfile		
RegisterAgent	Octroie l'autorisation d'enregistrer un agent	Écrire			
ReserveContact	Accorde l'autorisation de réserver un contact.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation d'attribuer une balise de ressource.	Identification	Config		
			Contact		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Octroie l'autorisation d'annuler l'attribution d'une balise de ressource.	Identification	Config		
			Contact		
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgentStatus	Octroie l'autorisation de mettre à jour le statut d'un agent	Écrire	Agent*		
UpdateConfig	Accorde l'autorisation de mettre à jour une configuration.	Écrire	Config*		
UpdateEphemeris	Accorde l'autorisation de mettre à jour un modèle d'e-mail	Écrire	EphemerisItem*		
UpdateMissionProfile	Accorde l'autorisation de mettre à jour un profil de mission.	Écrire	MissionProfile*		

Types de ressources définis par AWS Ground Station

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Config	`arn:${Partition}:groundstation:${Region}:${Account}:config/${ConfigType}/${ConfigId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
		groundstation:ConfigId groundstation:ConfigType
Contact	arn:${Partition}:groundstation:${Region}:${Account}:contact/${ContactId}	aws:ResourceTag/${TagKey} groundstation:ContactId
DataflowEndpointGroup	arn:${Partition}:groundstation:${Region}:${Account}:dataflow-endpoint-group/${DataflowEndpointGroupId}	aws:ResourceTag/${TagKey} groundstation:DataflowEndpointGroupId
EphemerisItem	arn:${Partition}:groundstation:${Region}:${Account}:ephemeris/${EphemerisId}	aws:ResourceTag/${TagKey} groundstation:EphemerisId
GroundStationResource	arn:${Partition}:groundstation:${Region}:${Account}:groundstation:${GroundStationId}	groundstation:GroundStationId
MissionProfile	arn:${Partition}:groundstation:${Region}:${Account}:mission-profile/${MissionProfileId}	aws:ResourceTag/${TagKey} groundstation:MissionProfileId
Satellite	arn:${Partition}:groundstation:${Region}:${Account}:satellite/${SatelliteId}	groundstation:SatelliteId

Types de ressources	ARN	Clés de condition
Agent	`arn:${Partition}:groundstation:${Region}:${Account}:agent/${AgentId}`	groundstation:AgentId

Clés de condition pour AWS Ground Station

AWS Ground Station définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
groundstation:AgentId	Filtre l'accès en fonction de l'ID d'un agent	String
groundstation:ConfigId	Filtre l'accès en fonction de l'ID d'une configuration.	Chaîne
groundstation:ConfigType	Filtre l'accès en fonction du type d'une configuration.	Chaîne

Clés de condition	Description	Type
groundstation:ContactId	Filtre l'accès en fonction de l'ID d'un contact.	Chaîne
groundstation:DataflowEndpointGroupId	Filtre l'accès en fonction de l'ID d'un groupe de points de terminaison de flux de données.	String
groundstation:EphemerisId	Filtre l'accès par l'ID d'une image.	String
groundstation:GroundStationId	Filtre l'accès en fonction de l'ID d'une station au sol.	Chaîne
groundstation:MissionProfileId	Filtre l'accès en fonction de l'ID d'un profil de mission.	Chaîne
groundstation:SatelliteId	Filtre l'accès en fonction de l'ID d'un satellite.	String

Actions, ressources et clés de condition pour Amazon GroundTruth Labeling

Amazon GroundTruth Labeling (préfixe de service :`groundtruthlabeling`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon GroundTruth Labeling
- Types de ressources définis par Amazon GroundTruth Labeling
- Clés de condition pour Amazon GroundTruth Labeling

Actions définies par Amazon GroundTruth Labeling

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociatePatchToManifestJob [autorisation uniquement]	Accorde l'autorisation d'associer un fichier correctif au fichier manifeste pour mettre à jour le fichier manifeste.	Écriture			
CreateBatch [autorisation uniquement]	Accorde l'autorisation de créer un GT+ Batch	Écrire			
CreateIntakeForm [autorisation uniquement]	Accorde l'autorisation de créer un formulaire d'admission	Écrire			
CreateProject [autorisa	Accorde l'autorisation de créer un projet GT+	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
tion uniquement]					
CreateWorkflowDefinition [autorisation uniquement]	Accorde l'autorisation de créer une définition de flux de travail GT+	Écrire			
DescribeConsoleJob [autorisation uniquement]	Donne l'autorisation d'obtenir le statut des GroundTruthLabeling emplois	Lecture			
GenerateLIDARPreviewTaskConfigJob [autorisation uniquement]	Accorde l'autorisation de générer une tâche de prévisualisation LiDAR	Écrire			
GetBatch [autorisation uniquement]	Accorde l'autorisation d'obtenir un GT+ Batch	Lecture			
GetIntakeFormStatus [autorisation uniquement]	Donne l'autorisation d'obtenir un formulaire d'admission	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBatches [autorisation uniquement]	Autorise la mise en vente d'un GT+ Batchs	Lecture			
ListDatasetObjects [autorisation uniquement]	Accorde l'autorisation de répertorier des objets de jeu de données dans un fichier manifeste.	Lecture			
ListProjects [autorisation uniquement]	Donne l'autorisation de répertorier un projet GT+	Lecture			
RunFilterOrSampleDatasetJob [autorisation uniquement]	Accorde l'autorisation de filtrer les enregistrements à partir d'un fichier manifeste à l'aide de S3 Select. Obtient des exemples d'entrées en fonction d'un échantillonnage aléatoire.	Écriture			
RunGenerateManifestByCrawlingJob [autorisation uniquement]	Accorde l'autorisation de répertorier un préfixe S3 et de créer des fichiers manifestes à partir d'objets à cet emplacement.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RunGenerateManifestMetricsJob [autorisation uniquement]	Accorde l'autorisation de générer des métriques à partir d'objets dans le manifeste	Écrire			
UpdateBatch [autorisation uniquement]	Autorise la mise à jour d'un GT + Batch	Écrire			

Types de ressources définis par Amazon GroundTruth Labeling

Amazon GroundTruth Labeling ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon GroundTruth Labeling, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Amazon GroundTruth Labeling

GroundTruth L'étiquetage ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon GuardDuty

Amazon GuardDuty (préfixe de service :`guardduty`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon GuardDuty
- Types de ressources définis par Amazon GuardDuty
- Clés de condition pour Amazon GuardDuty

Actions définies par Amazon GuardDuty

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptAdministratorInvitation	Accorde l'autorisation d'accepter des invitations pour devenir un compte GuardDuty membre	Écrire			
AcceptInvitation	Accorde l'autorisation d'accepter des invitations pour devenir un compte GuardDuty membre	Écrire			
ArchiveFindings	Autorise l'archivage des GuardDuty résultats	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDetector	Accorde l'autorisation de créer un détecteur	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateFilter	Accorde l'autorisation de créer des GuardDuty filtres. Un filtre définit les attributs et les conditions de résultat utilisés pour filtrer les résultats	Écrire	filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIPSet	Accorde l'autorisation de créer un IPSet	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMalwareProtectionPlan	Autorise la création d'un nouveau plan de protection contre les logiciels malveillants	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateMembers	Accorde l'autorisation de créer des comptes de GuardDuty membre, le compte utilisé pour créer un membre devenant le compte GuardDuty d'administrateur	Écrire			
CreatePublishingDestination	Accorde l'autorisation de créer une destination de publication	Écriture		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateSampleFindings	Accorde l'autorisation de créer des exemples de résultats.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateThreatEntitySet	Accorde l'autorisation de créer GuardDuty ThreatEntitySets, lorsqu'un ThreatEntitySet est constitué d'adresses IP malveillantes connues, des and/or domaines utilisés GuardDuty pour générer des résultats	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateThreatIntelSet	Accorde l'autorisation de créer GuardDuty ThreatIntelSets, lorsque a ThreatIntelSet est constitué d'adresses IP malveillantes connues utilisées GuardDuty pour générer des résultats	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrustedEntitySet	Accorde l'autorisation de créer un TrustedEntitySet	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
DeclineInvitations	Accorde l'autorisation de refuser les invitations à devenir un compte GuardDuty membre	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDetector	Autorise la suppression GuardDuty des détecteurs	Écrire	detector*		
DeleteFilter	Accorde l'autorisation de supprimer GuardDuty des filtres	Écrire	filter*		
DeleteIPSet	Accorde l'autorisation de suppression GuardDuty IPSets	Écrire	ipset*		
DeleteInvitations	Accorde l'autorisation de supprimer les invitations à devenir un compte GuardDuty membre	Écrire			
DeleteMalwareProtectionPlan	Autorise la suppression d'un plan de protection contre les programmes malveillants	Écrire	malwareprotectionplan*		
DeleteMembers	Accorde l'autorisation de supprimer les comptes des GuardDuty membres	Écrire			
DeletePublishingDestination	Accorde l'autorisation de supprimer une destination de publication	Écrire	publishingDestination*		
DeleteThreatEntitySet	Accorde l'autorisation de suppression GuardDuty ThreatEntitySets	Écrire	threatentityset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteThreatIntelSet	Accorde l'autorisation de suppression GuardDuty ThreatIntelSets	Écrire	threatintelset*		
DeleteTrustedEntitySet	Accorde l'autorisation de suppression GuardDuty TrustedEntitySets	Écrire	trustedentityset*		
DescribeMalwareScans	Accorde l'autorisation de récupérer des informations sur les analyses de logiciels malveillants	Lecture			
DescribeOrganizationConfiguration	Accorde l'autorisation de récupérer des informations sur l'administrateur délégué associé à un GuardDuty détecteur	Lecture			
DescribePublishingDestination	Accorde l'autorisation de récupérer les détails relatifs à une destination de publication	Lecture	publishingDestination*		
DisableOrganizationAdminAccount	Accorde l'autorisation de désactiver l'administrateur délégué de l'organisation pour GuardDuty	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateFromAdministratorAccount	Accorde l'autorisation de dissocier un compte GuardDuty membre de son compte GuardDuty administrateur	Écrire			
DisassociateFromMasterAccount	Accorde l'autorisation de dissocier un compte GuardDuty membre de son compte GuardDuty administrateur	Écrire			
DisassociateMembers	Accorde l'autorisation de dissocier GuardDuty les comptes des membres de leur compte administrateur GuardDuty	Écrire			
EnableOrganizationAdminAccount	Accorde l'autorisation d'activer l'administrateur délégué d'une organisation pour GuardDuty	Écrire			
GetAdministratorAccount	Accorde l'autorisation de récupérer les détails du compte GuardDuty administrateur associé à un compte membre	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCoverageStatistics	Accorde l'autorisation de répertorier les statistiques de GuardDuty couverture Amazon pour le GuardDuty compte spécifié dans une région	Lecture	detector*		
GetDetector	Donne l'autorisation de récupérer les GuardDuty détecteurs	Lecture	detector*		
GetFilter	Accorde l'autorisation de récupérer GuardDuty les filtres	Lecture	filter*		
GetFindings	Donne l'autorisation de récupérer les GuardDuty résultats	Lecture			
GetFindingsStatistics	Autorise l'extraction d'une liste de statistiques de GuardDuty recherche	Lecture			
GetIPSet	Accorde l'autorisation de récupérer GuardDuty IPSets	Lecture	ipset*		
GetInvitationsCount	Accorde l'autorisation de récupérer le nombre de toutes les GuardDuty invitations envoyées à un compte spécifié, ce qui n'inclut pas l'invitation acceptée	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMalwareProtectionPlan	Accorde l'autorisation de récupérer les détails d'un plan de protection contre les logiciels malveillants	Lecture	malwareprotectionplan*		
GetMalwareScan	Autorise à récupérer les détails d'une analyse de logiciels malveillants	Lecture			
GetMalwareScanSettings	Accorde l'autorisation de récupérer les paramètres de l'analyse des logiciels malveillants	Lecture			
GetMasterAccount	Accorde l'autorisation de récupérer les détails du compte GuardDuty administrateur associé à un compte membre	Lecture			
GetMemberDetectors	Accorde l'autorisation de décrire les sources de données activées pour les détecteurs de comptes membres	Lecture			
GetMembers	Accorde l'autorisation de récupérer les comptes membres associés à un compte d'administrateur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOrganizationStatistics	Accorde l'autorisation de récupérer les statistiques de couverture GuardDuty des plans de protection pour les comptes des membres dans une région	Lecture			
GetRemainingFreeTrialDays	Accorde l'autorisation de fournir le nombre de jours restants pour chaque source de données utilisée pendant la période d'essai gratuite	Lecture			
GetThreatEntitySet	Accorde l'autorisation de récupérer GuardDuty ThreatEntitySets	Lecture	threatentityset*		
GetThreatIntelSet	Accorde l'autorisation de récupérer GuardDuty ThreatIntelSets	Lecture	threatintelset*		
GetTrustedEntitySet	Accorde l'autorisation de récupérer GuardDuty TrustedEntitySets	Lecture	trustedentityset*		
GetUsageStatistics	Autorise à répertorier les statistiques GuardDuty d'utilisation d'Amazon au cours des 30 derniers jours pour l'ID de détecteur spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InviteMembers	Accorde l'autorisation d'inviter d'autres AWS comptes à activer GuardDuty et à devenir des comptes GuardDuty membres	Écrire			
ListCoverage	Accorde l'autorisation de répertorier tous les détails des ressources d'un compte donné dans une région	List	detector*		
ListDetectors	Autorise la récupération d'une liste de GuardDuty détecteurs	List			
ListFilters	Accorde l'autorisation de récupérer une liste de GuardDuty filtres	List			
ListFindings	Autorise la récupération d'une liste de GuardDuty résultats	List			
ListIPSets	Accorde l'autorisation de récupérer une liste de GuardDuty IPSets	List			
ListInvitations	Accorde l'autorisation de récupérer une liste de toutes les invitations GuardDuty d'adhésion envoyées à un Compte AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMalwareProtectionPlans	Autorise la récupération d'une liste de plans de protection contre les programmes malveillants	List			
ListMalwareScans	Autorise la récupération d'une liste d'analyses de logiciels malveillants	List			
ListMembers	Accorde l'autorisation de récupérer la liste des comptes de GuardDuty membres associés à un compte d'administrateur	List			
ListOrganizationAdminAccounts	Accorde l'autorisation de répertorier les informations relatives à l'administrateur délégué de l'organisation pour GuardDuty	List			
ListPublishingDestinations	Accorde l'autorisation de récupérer une liste de destinations de publication	List			
ListTagsForResource	Accorde l'autorisation de récupérer une liste de balises associées à une GuardDuty ressource	Lecture	detector		
			filter		
			ipset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			malwareprotectionplan		
			publishingDestination		
			threatentityset		
			threatintelset		
			trustedentityset		
ListThreatEntitySets	Accorde l'autorisation de récupérer une liste de GuardDuty ThreatEntitySets	List			
ListThreatIntelSets	Accorde l'autorisation de récupérer une liste de GuardDuty ThreatIntelSets	List			
ListTrustedEntitySets	Accorde l'autorisation de récupérer une liste de GuardDuty TrustedEntitySets	List			
SendObjectMalwareScan	Autorise le lancement d'une nouvelle analyse des malwares liés aux objets	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendSecurityTelemetry	Accorde l'autorisation d'envoyer des données de télémétrie de sécurité pour un GuardDuty compte spécifique dans une région	Écrire			
StartMalwareScan	Accorde l'autorisation de lancer une nouvelle analyse de logiciels malveillants	Écrire			
StartMonitoringMembers	Autorise un compte GuardDuty administrateur à suivre les résultats des comptes des GuardDuty membres	Écrire			
StopMonitoringMembers	Accorde l'autorisation de désactiver les résultats de la surveillance des comptes membres	Écrire			
TagResource	Accorde l'autorisation d'ajouter des balises à une GuardDuty ressource	Identification	detector		
			filter		
			ipset		
			malwareprotectionplan		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			publishingDestination		
			threatentityset		
			threatintelset		
			trustedentityset		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unarchive Findings	Accorde l'autorisation de désarchiver les résultats GuardDuty	Écrire			
UntagResource	Accorde l'autorisation de supprimer des balises d'une GuardDuty ressource	Identification	detector		
			filter		
			ipset		
			malwareprotectionplan		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			publishingDestination		
			threatentityset		
			threatintelset		
			trustedentityset		
				aws:TagKeys	
UpdateDetector	Autorise la mise à jour GuardDuty des détecteurs	Écrire	detector*		
UpdateFilter	Accorde l'autorisation de mettre à jour GuardDuty les filtres	Écrire	filter*		
UpdateFindingsFeedback	Accorde l'autorisation de mettre à jour les commentaires sur GuardDuty les résultats pour marquer les résultats comme utiles ou non utiles	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateIPSet	Accorde l'autorisation de mise à jour GuardDuty IPSets	Écrire	ipset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMalwareProtectionPlan	Autorise la mise à jour du plan de protection contre les logiciels malveillants	Écrire	malwareprotectionplan*		
UpdateMalwareScanSettings	Accorde l'autorisation de mettre à jour les paramètres de l'analyse des logiciels malveillants	Écrire			
UpdateMemberDetectors	Accorde l'autorisation de mettre à jour les sources de données activées pour les détecteurs de comptes membres	Écrire			
UpdateOrganizationConfiguration	Accorde l'autorisation de mettre à jour la configuration d'administrateur délégué associée à un GuardDuty détecteur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePublishingDestination	Accorde l'autorisation de mettre à jour une destination de publication	Écrire	publishingDestination*		s3:GetObject s3:ListBucket
UpdateThreatEntitySet	Accorde l'autorisation de mise à jour GuardDuty ThreatEntitySets	Écrire	threatentityset*		s3:GetObject
UpdateThreatIntelSet	Accorde l'autorisation de mettre à jour le GuardDuty ThreatIntelSets	Écrire	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateTrustedEntitySet	Accorde l'autorisation de mise à jour GuardDuty TrustedEntitySets	Écrire	trustedentityset*		s3:GetObject

Types de ressources définis par Amazon GuardDuty

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
detector	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}	aws:ResourceTag/${TagKey}
filter	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}	aws:ResourceTag/${TagKey}
ipset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}	aws:ResourceTag/${TagKey}
threatintelset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}	aws:ResourceTag/${TagKey}
trustedentityset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/trustedentityset/${TrustedEntitySetId}	aws:ResourceTag/${TagKey}
threatentityset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatentityset/${ThreatEntitySetId}	aws:ResourceTag/${TagKey}
publishingDestination	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/publishingdestination/${PublishingDestinationId}	aws:ResourceTag/${TagKey}
malwareprotectionplan	arn:${Partition}:guardduty:${Region}:${Account}:malware-protection-plan/${MalwareProtectionPlanId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon GuardDuty

Amazon GuardDuty définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de balise dans la requête.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString

Actions, ressources et clés de condition pour AWS Health APIs and Notifications

AWS Health APIs and Notifications (préfixe de service :`health`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Health APIs and Notifications

- Types de ressources définis par AWS Health APIs and Notifications
- Clés de condition pour AWS Health APIs and Notifications

Actions définies par AWS Health APIs and Notifications

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAffectedAccountsForOrganization	Accorde l'autorisation de récupérer une liste de comptes qui ont été affectés par les événements spécifiés dans l'organisation	Lecture			organizations:ListAccounts
DescribeAffectedEntities	Accorde l'autorisation de récupérer une liste d'entités qui ont été affectées par les événements spécifiés	Lecture	event*		
				health:eventTypeCode health:service	
DescribeAffectedEntitiesForOrganization	Accorde l'autorisation de récupérer une liste d'entités qui ont été affectées par les événements et les comptes spécifiés dans l'organisation	Lecture			organizations:ListAccounts

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEntityAggregates	Accorde l'autorisation de récupérer le nombre d'entités qui sont affectées par chacun des événements spécifiés	Lecture			
DescribeEntityAggregatesForOrganization	Accorde l'autorisation de récupérer le nombre d'entités qui sont affectées par chacun des événements spécifiés dans une organisation	Lecture			organizations:ListAccounts
DescribeEventAggregates	Accorde l'autorisation de récupérer le nombre d'événements par type d'événement (problème, modification planifiée et notification de compte)	Lecture			
DescribeEventDetails	Accorde l'autorisation de récupérer des informations détaillées sur un ou plusieurs événements spécifiés	Lecture	event*		
				health:eventTypeCode health:service	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEventDetailsForOrganization	Accorde l'autorisation de récupérer des informations détaillées sur un ou plusieurs événements spécifiés pour les comptes fournis dans l'organisation	Lecture			organizations:ListAccounts
DescribeEventTypes	Accorde l'autorisation de récupérer les types d'événements répondant aux critères de filtrage spécifiés	Lecture			
DescribeEvents	Accorde l'autorisation de récupérer des informations sur des événements répondant aux critères de filtrage spécifiés	Lecture			
DescribeEventsForOrganization	Accorde l'autorisation de récupérer des informations sur les événements répondant aux critères de filtrage spécifiés dans l'organisation	Lecture			organizations:ListAccounts
DescribeHealthServiceStatusForOrganization	Accorde l'autorisation de récupérer le statut d'activation ou de désactivation de la fonction Vue organisationnelle	Lecture			organizations:ListAccounts

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableHealthServiceAccessForOrganization	Accorde l'autorisation de désactiver la fonction Vue organisationnelle	Gestion des autorisations			organizations:DisableAWSServiceAccess organizations:ListAccounts
EnableHealthServiceAccessForOrganization	Accorde l'autorisation d'activer la fonction de vue organisationnelle	Gestion des autorisations			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:ListAccounts

Types de ressources définis par AWS Health APIs and Notifications

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
event	`arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*`	

Clés de condition pour AWS Health APIs and Notifications

AWS Health APIs and Notifications définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
health:eventTypeCode	Filtre l'accès en fonction du type d'événement	String
health:service	Filtre l'accès en fonction du service impacté	String

Actions, ressources et clés de condition pour AWS HealthImaging

AWS HealthImaging (préfixe de service :`medical-imaging`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS HealthImaging
- Types de ressources définis par AWS HealthImaging
- Clés de condition pour AWS HealthImaging

Actions définies par AWS HealthImaging

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CopyImageSet	Octroie l'autorisation de copier un ensemble d'images.	Écrire	datastore*		
			imageset*		
CreateDatastore	Octroie l'autorisation de créer un entrepôt de données pour ingérer des données d'imagerie.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatastore	Octroie l'autorisation de supprimer un entrepôt de données.	Écrire	datastore*		
DeleteImageSet	Octroie l'autorisation de supprimer un ensemble d'images.	Écrire	datastore*		
			imageset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDICOMBulkdata	Accorde l'autorisation d'obtenir des données en masse dicom au format binaire	Lecture	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	
GetDICOMImportJob	Octroie l'autorisation d'obtenir les propriétés d'une tâche d'importation.	Lecture	datastore*		
GetDICOMInstance	Accorde l'autorisation d'obtenir une instance dicom au format dcm	Lecture	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDICOMInstanceFrames	Accorde l'autorisation d'obtenir des cadres d'instance dicom dans le format demandé par le client	Lecture	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	
GetDICOMInstanceMetadata	Accorde l'autorisation d'obtenir les métadonnées d'une instance dicom au format DICOM JSON	Lecture	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDICOMSeriesMetadata	Accorde l'autorisation de récupérer les métadonnées pour toutes les instances DICOM appartenant à une série DICOM donnée au format DICOM JSON	Lecture	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	
GetDatastore	Octroie l'autorisation d'obtenir les propriétés de l'entrepôt de données.	Lecture	datastore*		
GetImageFrame	Octroie l'autorisation d'obtenir les propriétés du cadre d'image.	Lecture	datastore*		
			imageset*		
GetImageSet	Octroie l'autorisation d'obtenir les propriétés de l'ensemble d'images.	Lecture	datastore*		
			imageset*		
GetImageSetMetadata	Octroie l'autorisation d'obtenir les propriétés de métadonnées de l'ensemble d'images.	Lecture	datastore*		
			imageset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDICOMImportJobs	Octroie l'autorisation de répertorier les tâches d'importation pour un entrepôt de données.	List	datastore*		
ListDatastores	Octroie l'autorisation de répertorier les entrepôts de données.	List			
ListImageSetVersions	Octroie l'autorisation de répertorier les versions d'un ensemble d'images.	List	datastore*		
			imageset*		
ListTagsForResource	Octroie l'autorisation de répertorier les balises d'une ressource d'imagerie médicale.	List	datastore		
			imageset		
SearchDICOMInstances	Accorde l'autorisation de rechercher des instances dicom qui renvoient des données au format DICOM JSON	Lecture	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchDICOMSeries	Autorise la recherche dans les séries dicom qui renvoient des données au format DICOM JSON	Lecture	datastore*		
				medical-imaging:StudyInstanceUID	
SearchDICOMStudies	Autorise la recherche dans les études dicom qui renvoient des données au format DICOM JSON	Lecture	datastore*		
SearchImageSets	Octroie l'autorisation de rechercher des ensembles d'images.	Lecture	datastore*		
StartDICOMImportJob	Octroie l'autorisation de lancer une tâche d'importation DICOM.	Écrire	datastore*		
StoreDICOM	Accorde l'autorisation de stocker les instances dicom qui renvoient le résultat au format DICOM JSON	Écrire	datastore*		
StoreDICOMStudy	Autorise le stockage d'une étude dicom qui renvoie le résultat au format DICOM JSON	Écrire	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				medical-imaging:StudyInstanceUID	
TagResource	Octroie l'autorisation d'ajouter des balises à une ressource d'imagerie médicale.	Identification	datastore		
			imageset		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Octroie l'autorisation de supprimer les balises d'une ressource d'imagerie médicale.	Identification	datastore		
			imageset		
				aws:TagKeys	
UpdateImageSetMetadata	Octroie l'autorisation de mettre à jour les propriétés de métadonnées de l'ensemble d'images.	Écrire	datastore*		
			imageset*		

Types de ressources définis par AWS HealthImaging

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
datastore	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}`	aws:ResourceTag/${TagKey}
imageset	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}/imageset/${ImageSetId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS HealthImaging

AWS HealthImaging définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
medical-imaging:SeriesInstanceUID	Filtre l'accès en fonction du paramètre SeriesInstance UID dans la demande	String
medical-imaging:StudyInstanceUID	Filtre l'accès en fonction du paramètre StudyInstance UID dans la demande	String

Actions, ressources et clés de condition pour AWS HealthLake

AWS HealthLake (préfixe de service :`healthlake`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS HealthLake
- Types de ressources définis par AWS HealthLake
- Clés de condition pour AWS HealthLake

Actions définies par AWS HealthLake

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelFHIRExportJobWithDelete	Accorde l'autorisation d'annuler une tâche d'exportation FHIR en cours avec Delete	Écrire	datastore*		
ConfirmAttributionList	Accorde l'autorisation aux clients d'indiquer à un producteur que le consommateur n'a plus aucune modification à apporter à la liste d'attribution	Écrire	datastore*		
CreateFHIRDatastore	Accorde l'autorisation de créer un magasin de données capable d'ingérer et d'exporter des données FHIR	Écriture		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateResource	Accorde l'autorisation de créer une ressource	Écriture	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFHIRDatastore	Accorde l'autorisation de supprimer un magasin de données	Écriture	datastore*		
DeleteResource	Accorde l'autorisation de supprimer une ressource	Écrire	datastore*		
DescribeFHIRBulkDeleteJob	Accorde l'autorisation de décrire un Job FHIR Bulk Delete	Lecture	datastore*		
DescribeFHIRBulkMemberMatchJob	Accorde l'autorisation de décrire un job FHIR Bulk Member Match	Lecture	datastore*		
DescribeFHIRDatastore	Accorde l'autorisation d'obtenir les propriétés associées au magasin de données FHIR, y compris l'ID, l'ARN, le nom, le statut du magasin de données, l'emplacement de création, la version du type de magasin de données et le point de terminaison du magasin de données	Lecture	datastore*		
DescribeFHIRExportJob	Accorde l'autorisation d'afficher les propriétés d'une tâche d'exportation FHIR, y compris l'ID, l'ARN, le nom et le statut du magasin de données	Lecture	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFHIRExportJobWithGet	Accorde l'autorisation d'afficher les propriétés d'une tâche d'exportation FHIR, notamment l'ID, l'ARN, le nom et le statut de la banque de données avec Get	Lecture	datastore*		
DescribeFHIRImportJob	Accorde l'autorisation d'afficher les propriétés d'une tâche d'importation FHIR, y compris l'ID, l'ARN, le nom et le statut du magasin de données	Lecture	datastore*		
ExpandValueSetWithGet	Accorde l'autorisation de rechercher et d'étendre les ValueSet ressources	Lecture	datastore*		
ExpandValueSetWithPost	Accorde l'autorisation de rechercher et d'étendre les ValueSet ressources	Lecture	datastore*		
GenerateDocumentWithGet	Autorise la génération d'une ressource documentaire clinique	Écrire	datastore*		
GenerateDocumentWithPost	Autorise la génération d'une ressource documentaire clinique	Écrire	datastore*		
GetCapabilities	Accorde l'autorisation d'obtenir les capacités d'un magasin de données FHIR	Lecture	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExportedFile	Accorde l'autorisation d'accéder aux fichiers exportés à partir d'une tâche d'exportation FHIR initiée avec Get	Lecture	datastore*		
GetHistoryByResourceId	Autorise la lecture de l'historique des ressources	Lecture	datastore*		
InquirePreAuthClaim	Accorde l'autorisation de se renseigner sur le statut d'une demande d'autorisation préalable	Lecture	datastore*		
ListFHIRDatastores	Accorde l'autorisation de répertorier toutes les banques de données FHIR présentes dans le compte de l'utilisateur, quel que soit le statut de la banque de données	List			
ListFHIRExportJobs	Accorde l'autorisation d'obtenir une liste de tâches d'exportation pour le magasin de données spécifié	Liste	datastore*		
ListFHIRImportJobs	Accorde l'autorisation d'obtenir une liste de tâches d'importation pour le magasin de données spécifié	Liste	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation d'obtenir une liste de balises pour le magasin de données spécifié	List	datastore		
LookupCodeSystemWithGet	Accorde l'autorisation de récupérer les codes d'une CodeSystem ressource	Lecture	datastore*		
LookupCodeSystemWithPost	Accorde l'autorisation de récupérer les codes d'une CodeSystem ressource	Lecture	datastore*		
MemberAdd	Accorde l'autorisation d'attribuer à un membre un groupe de fournisseurs spécifique	Écrire	datastore*		
MemberMatch	Accorde l'autorisation de permettre le jumelage des patients entre les systèmes	Écrire	datastore*		
MemberRemove	Accorde l'autorisation de supprimer un membre d'un groupe.	Écrire	datastore*		
PatchResource	Accorde l'autorisation de patcher une ressource	Écrire	datastore*		
ProcessBundle	Accorde l'autorisation de regrouper plusieurs opérations sur les ressources	Écrire	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
QuestionnairePackage	Accorde l'autorisation de récupérer des packages de questionnaires avec bibliothèque de dépendances et ValueSet ressources	Lecture	datastore*		
ReadResource	Accorde l'autorisation de lire une ressource	Lecture	datastore*		
RetrieveAttributionStatus	Accorde l'autorisation de récupérer le statut d'attribution des membres	Écrire	datastore*		
SearchEverything	Autorise la recherche de toutes les ressources relatives à un patient	Lecture	datastore*		
SearchWithGet	Accorde l'autorisation de rechercher des ressources avec la méthode GET	Lecture	datastore*		
SearchWithPost	Accorde l'autorisation de rechercher des ressources avec la méthode POST	Lecture	datastore*		
StartFHIRBulkDeleteJob	Autorise le lancement d'une tâche FHIR Bulk Delete	Écrire	datastore*		
StartFHIRBulkMemberMatchJob	Donne l'autorisation de commencer un job FHIR Bulk Member Match	Écrire	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartFHIRExportJob	Accorde l'autorisation de démarrer une tâche d'exportation FHIR	Écrire	datastore*		
StartFHIRExportJobWithGet	Donne l'autorisation de commencer un travail d'exportation FHIR avec Get	Écrire	datastore*		
StartFHIRExportJobWithPost	Donne l'autorisation de commencer un travail d'exportation chez FHIR avec Post	Écrire	datastore*		
StartFHIRImportJob	Accorde l'autorisation de démarrer une tâche d'importation FHIR	Écrire	datastore*		
SubmitPreAuthClaim	Accorde l'autorisation de soumettre une demande d'autorisation préalable	Écrire	datastore*		
TagResource	Accorde l'autorisation d'ajouter des balises à un magasin de données	Balisage	datastore		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer les balises associées à un magasin de données	Balisage	datastore		
				aws:TagKeys	
UpdateResource	Accorde l'autorisation de mettre à jour des ressources	Écrire	datastore*		
ValidateResource	Accorde l'autorisation de valider une ressource	Lecture	datastore*		
VersionReadResource	Accorde l'autorisation de lire la version d'une ressource	Lecture	datastore*		

Types de ressources définis par AWS HealthLake

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
datastore	`arn:${Partition}:healthlake:${Region}:${Account}:datastore/fhir/${DatastoreId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS HealthLake

AWS HealthLake définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS HealthOmics

AWS HealthOmics (préfixe de service :`omics`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS HealthOmics
- Types de ressources définis par AWS HealthOmics
- Clés de condition pour AWS HealthOmics

Actions définies par AWS HealthOmics

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AbortMultipartReadSetUpload	Accorde l'autorisation d'abandonner les chargements partitionnés de jeux de lecture	Écrire	sequenceStore*		
AcceptShare	Accorde l'autorisation d'accepter un partage	Écrire			
BatchDeleteReadSet	Accorde l'autorisation de supprimer par lots des jeux de lecture dans le magasin de séquences donné	Écrire	sequenceStore*		
CancelAnnotationImportJob	Accorde l'autorisation d'annuler une tâche d'importation d'annotations	Écrire			
CancelRun	Accorde l'autorisation d'annuler l'exécution d'un flux de travail et d'arrêter toutes les tâches du flux de travail	Écrire	run*		
CancelVariantImportJob	Accorde l'autorisation d'annuler une tâche d'importation de variantes	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CompleteMultipartReadSetUpload	Accorde l'autorisation de terminer un chargement partitionné de jeux de lecture	Écrire	sequenceStore*		
CreateAnnotationStore	Accorde l'autorisation de créer un magasin d'annotations	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnnotationStoreVersion	Accorde l'autorisation de créer une version dans un magasin d'annotations	Écrire	AnnotationStore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	Accorde l'autorisation de créer une nouvelle configuration	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeSecurityGroups ec2:DescribeSubnets iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMultipartReadSetUpload	Accorde l'autorisation de créer un chargement partitionné de jeux de lecture	Écrire	sequenceStore*		
CreateReferenceStore	Accorde l'autorisation de créer un magasin de références	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunCache	Accorde l'autorisation de créer un nouveau cache d'exécution du flux de travail	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunGroup	Accorde l'autorisation de créer un groupe d'exécution de flux de travail	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSequenceStore	Accorde l'autorisation de créer un magasin de séquences	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateShare	Accorde l'autorisation de créer un partage	Écrire			
CreateVariantStore	Accorde l'autorisation de créer un magasin de variantes	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflow	Accorde l'autorisation de créer un flux de travail avec une définition de flux de travail et un modèle de paramètres de flux de travail	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowVersion	Accorde l'autorisation de créer une nouvelle version de flux de travail avec une définition de flux de travail et un modèle de paramètres de flux de travail	Écrire	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnnotationStore	Accorde l'autorisation de supprimer un magasin d'annotations	Écrire	AnnotationStore*		
DeleteAnnotationStoreVersions	Accorde l'autorisation de supprimer des versions d'un magasin d'annotations	Écrire	AnnotationStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			AnnotationStoreVersion*		
DeleteConfiguration	Accorde l'autorisation de supprimer une configuration	Écrire	configuration*		
DeleteReference	Accorde l'autorisation de supprimer une référence dans le magasin de références donné	Écrire	reference*		
			referenceStore*		
DeleteReferenceStore	Accorde l'autorisation de supprimer un magasin de références	Écrire	referenceStore*		
DeleteRun	Accorde l'autorisation de supprimer une exécution de flux de travail	Écrire	run*		
DeleteRunCache	Accorde l'autorisation de supprimer le cache d'exécution d'un flux de travail	Écrire	runCache*		
DeleteRunGroup	Accorde l'autorisation de supprimer un groupe d'exécution de flux de travail	Écrire	runGroup*		
DeleteS3AccessPolicy	Accorde l'autorisation de supprimer une politique d'accès sur un magasin donné	Écrire	sequenceStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSequenceStore	Accorde l'autorisation de supprimer un magasin de séquences	Écrire	sequenceStore*		
DeleteShare	Accorde l'autorisation de supprimer un partage	Écrire			
DeleteVariantStore	Accorde l'autorisation de supprimer un magasin de variantes	Écrire	VariantStore*		
DeleteWorkflow	Accorde l'autorisation de supprimer un flux de travail.	Écrire	workflow*		
DeleteWorkflowVersion	Accorde l'autorisation de supprimer une version du flux de travail	Écrire	WorkflowVersion*		
			workflow*		
GetAnnotationImportJob	Accorde l'autorisation d'obtenir le statut d'une tâche d'importation d'annotations	Lecture			
GetAnnotationStore	Accorde l'autorisation d'obtenir des informations détaillées sur un magasin d'annotations	Lecture	AnnotationStore*		
GetAnnotationStoreVersion	Accorde l'autorisation d'obtenir des informations détaillées sur une version d'un magasin d'annotations	Lecture	AnnotationStoreVersion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConfiguration	Accorde l'autorisation de récupérer les détails de configuration	Lecture	configuration*		
GetReadSet	Accorde l'autorisation d'obtenir un jeu de lecture dans le magasin de séquences donné	Lecture	readSet*		
			sequenceStore*		
GetReadSetActivationJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'activation d'un jeu de lecture pour le magasin de séquences donné	Lecture	sequenceStore*		
GetReadSetExportJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'exportation d'un jeu de lecture pour le magasin de séquences donné	Lecture	sequenceStore*		
GetReadSetImportJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'importation d'un jeu de lecture pour le magasin de séquences donné	Lecture	sequenceStore*		
GetReadSetMetadata	Accorde l'autorisation d'obtenir des informations sur un jeu de lecture dans le magasin de séquences donné	Lecture	readSet*		
			sequenceStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetReference	Accorde l'autorisation d'obtenir une référence dans le magasin de références donné	Lecture	reference*		
			referenceStore*		
GetReferenceImportJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'importation d'une référence pour le magasin de séquences donné	Lecture	referenceStore*		
GetReferenceMetadata	Accorde l'autorisation d'obtenir des informations sur une référence dans le magasin de séquences donné	Lecture	reference*		
			referenceStore*		
GetReferenceStore	Accorde l'autorisation d'obtenir des informations sur un magasin de références	Lecture	referenceStore*		
GetRun	Accorde l'autorisation de récupérer les informations de l'exécution du flux de travail	Lecture	run*		
GetRunCache	Accorde l'autorisation de récupérer les détails du cache d'exécution du flux de travail	Lecture	runCache*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRunGroup	Accorde l'autorisation de récupérer les informations du groupe de l'exécution du flux de travail	Lecture	runGroup*		
GetRunTask	Accorde l'autorisation de récupérer les informations des tâches du flux de travail	Lecture	TaskResource*		
			run*		
GetS3AccessPolicy	Accorde l'autorisation d'obtenir des informations sur une politique d'accès sur une boutique donnée	Lecture	sequenceStore*		
GetSequenceStore	Accorde l'autorisation d'obtenir des informations sur un magasin de séquences	Lecture	sequenceStore*		
GetShare	Accorde l'autorisation d'obtenir des informations détaillées sur un partage	Lecture			
GetVariantImportJob	Accorde l'autorisation d'obtenir le statut d'une tâche d'importation de variantes	Lecture			
GetVariantStore	Accorde l'autorisation d'obtenir des informations détaillées sur un magasin de variantes	Lecture	VariantStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkflow	Accorde l'autorisation de récupérer les informations du flux de travail	Lecture	workflow*		
GetWorkflowVersion	Accorde l'autorisation de récupérer les détails de la version du flux de travail	Lecture	WorkflowVersion*		
			workflow*		
ListAnnotationImportJobs	Accorde l'autorisation d'obtenir une liste des tâches d'importations d'annotations	List			
ListAnnotationStoreVersions	Accorde l'autorisation de récupérer une liste d'informations sur les versions d'un magasin d'annotations	List	AnnotationStore*		
ListAnnotationStores	Accorde l'autorisation de récupérer une liste d'informations sur les magasins d'annotations	List			
ListConfigurations	Accorde l'autorisation de récupérer une liste de configurations	List			
ListMultipartReadSetUploads	Accorde l'autorisation de répertorier les chargements partitionnés de jeux de lecture	List	sequenceStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListReadSetActivationJobs	Accorde l'autorisation de répertorier les tâches d'activation d'un jeu de lecture pour le magasin de séquences donné	List	sequenceStore*		
ListReadSetExportJobs	Accorde l'autorisation de répertorier les tâches d'exportation d'un jeu de lecture pour le magasin de séquences donné	List	sequenceStore*		
ListReadSetImportJobs	Accorde l'autorisation de répertorier les tâches d'importation d'un jeu de lecture pour le magasin de séquences donné	List	sequenceStore*		
ListReadSetUploadParts	Accorde l'autorisation de répertorier les parties des chargements partitionnés de jeux de lecture	List	sequenceStore*		
ListReadSets	Accorde l'autorisation de répertorier des jeux de lecture dans le magasin de séquences donné	List	sequenceStore*		
ListReferenceImportJobs	Accorde l'autorisation de répertorier des tâches d'importation de références pour le magasin de séquences donné	List	referenceStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListReferenceStores	Accorde l'autorisation de répertorier les magasins de références	List			
ListReferences	Accorde l'autorisation de répertorier les références dans le magasin de références donné	List	referenceStore*		
ListRunCaches	Accorde l'autorisation de récupérer une liste des caches d'exécution des flux de travail	List			
ListRunGroups	Accorde l'autorisation de récupérer une liste de groupes d'exécution de flux de travail	List			
ListRunTasks	Accorde l'autorisation de récupérer une liste de tâches pour une exécution de flux de travail	List	run*		
ListRuns	Accorde l'autorisation de récupérer une liste d'exécutions de flux de travail	List			
ListSequenceStores	Accorde l'autorisation de répertorier les magasins de séquences	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListShares	Accorde l'autorisation de récupérer une liste d'informations sur les partages	List			
ListTagsForResource	Accorde l'autorisation de récupérer une liste de AWS balises de ressources	List			
ListVariantImportJobs	Accorde l'autorisation d'obtenir une liste des tâches d'importation de variantes	List			
ListVariantStores	Accorde l'autorisation de récupérer une liste de métadonnées pour les magasins de variantes	List			
ListWorkflowVersions	Accorde l'autorisation de récupérer la liste des versions disponibles pour un flux de travail	List	workflow*		
ListWorkflows	Accorde l'autorisation de récupérer une liste de flux de travail disponibles	List			
PutS3AccessPolicy	Accorde l'autorisation d'appliquer une politique d'accès à un magasin donné	Écrire	sequenceStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartAnnotationImportJob	Accorde l'autorisation d'importer une liste de fichiers d'annotation dans un magasin d'annotations	Écrire	AnnotationStore*		
			AnnotationStoreVersion*		
StartReadSetActivationJob	Accorde l'autorisation de démarrer une tâche d'activation d'un jeu de lecture à partir du magasin de séquences donné	Écrire	sequenceStore*		
StartReadSetExportJob	Accorde l'autorisation de démarrer une tâche d'exportation d'un jeu de lecture à partir du magasin de séquences donné	Écrire	sequenceStore*		
StartReadSetImportJob	Accorde l'autorisation de démarrer une tâche d'importation d'un jeu de lecture dans le magasin de séquences donné	Écrire	sequenceStore*		
StartReferenceImportJob	Accorde l'autorisation de démarrer une tâche d'importation de références dans le magasin de séquences donné	Écrire	referenceStore*		
StartRun	Accorde l'autorisation de lancer un flux de travail	Écrire	run*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			configuration		
			runCache		
			runGroup		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVariantImportJob	Accorde l'autorisation d'importer une liste de fichiers de variantes dans un magasin de variantes	Écrire	VariantStore*		
TagResource	Accorde l'autorisation d'ajouter des AWS balises à une ressource	Identification	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			configuration		
			readSet		
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les AWS balises de ressources	Identification	AnnotationStore		
			AnnotationStoreVersion		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			VariantStore		
			WorkflowVersion		
			configuration		
			readSet		
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:TagKeys	
UpdateAnnotationStore	Accorde l'autorisation de mettre à jour les informations sur le magasin d'annotations	Écrire	AnnotationStore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAnnotationStoreVersion	Accorde l'autorisation de mettre à jour les informations sur une version dans un magasin d'annotations	Écrire	AnnotationStoreVersion*		
UpdateRunCache	Accorde l'autorisation de mettre à jour le cache d'exécution d'un flux de travail	Écrire	runCache*		
UpdateRunGroup	Accorde l'autorisation de mettre à jour un groupe d'exécution de flux de travail	Écrire	runGroup*		
UpdateSequenceStore	Autorise la mise à jour des informations relatives à un magasin de séquences	Écrire	sequenceStore*		
UpdateVariantStore	Accorde l'autorisation de mettre à jour les métadonnées du magasin de variantes	Écrire	VariantStore*		
UpdateWorkflow	Accorde l'autorisation de mettre à jour les informations d'un flux de travail	Écrire	workflow*		
UpdateWorkflowVersion	Autorise la mise à jour des détails de la version du flux de travail	Écrire	WorkflowVersion*		
			workflow*		
UploadReadSetPart	Accorde l'autorisation de charger les parties d'un jeu de lecture	Écrire	sequenceStore*		

Types de ressources définis par AWS HealthOmics

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AnnotationStore	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}`	aws:ResourceTag/${TagKey}
AnnotationStoreVersion	`arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}/version/${AnnotationStoreVersionName}`	aws:ResourceTag/${TagKey}
configuration	`arn:${Partition}:omics:${Region}:${Account}:configuration/${Name}`	aws:ResourceTag/${TagKey}
readSet	`arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}/readSet/${ReadSetId}`	aws:ResourceTag/${TagKey}
reference	`arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}/reference/${ReferenceId}`	aws:ResourceTag/${TagKey}
referenceStore	`arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}`	aws:ResourceTag/${TagKey}
run	`arn:${Partition}:omics:${Region}:${Account}:run/${Id}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
runCache	arn:${Partition}:omics:${Region}:${Account}:runCache/${Id}	aws:ResourceTag/${TagKey}
runGroup	arn:${Partition}:omics:${Region}:${Account}:runGroup/${Id}	aws:ResourceTag/${TagKey}
sequenceStore	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}	aws:ResourceTag/${TagKey}
TaskResource	arn:${Partition}:omics:${Region}:${Account}:task/${Id}	
VariantStore	arn:${Partition}:omics:${Region}:${Account}:variantStore/${VariantStoreName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}	aws:ResourceTag/${TagKey}
WorkflowVersion	arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}/version/${VersionName}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS HealthOmics

AWS HealthOmics définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Honeycode

Amazon Honeycode (préfixe de service : `honeycode`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Honeycode
- Types de ressources définis par Amazon Honeycode
- Clés de condition pour Amazon Honeycode

Actions définies par Amazon Honeycode

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApproveTeamAssociation [autorisation uniquement]	Accorde l'autorisation d'approuver une demande d'association d'équipe pour votre AWS compte	Écrire			
BatchCreateTableRows	Accorde l'autorisation de créer de nouvelles lignes dans une table.	Écriture	table*		
BatchDeleteTableRows	Accorde l'autorisation de supprimer des lignes d'une table.	Écriture	table*		
BatchUpdateTableRows	Accorde l'autorisation de mettre à jour des lignes dans une table.	Écriture	table*		
BatchUpsertTableRows	Accorde l'autorisation de fusionner des lignes dans une table.	Écriture	table*		
CreateTeam [autorisation uniquement]	Autorise la création d'une nouvelle équipe Amazon Honeycode pour votre compte AWS	Écrire			
CreateTenant [autorisation uniquement]	Autorise la création d'un nouveau locataire dans Amazon Honeycode pour votre compte AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDomains [autorisation uniquement]	Autorise la suppression de domaines Amazon Honeycode pour votre compte AWS	Écrire			
DeregisterGroups [autorisation uniquement]	Accorde l'autorisation de supprimer des groupes d'une équipe Amazon Honeycode pour votre compte AWS	Écrire			
DescribeTableDataImportJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'importation de données de table.	Lecture	table*		
DescribeTeam [autorisation uniquement]	Accorde l'autorisation d'obtenir des informations sur les équipes Amazon Honeycode pour votre compte AWS	Lecture			
GetScreenData	Accorde l'autorisation de charger les données à partir d'un écran	Lecture	screen*		
InvokeScreenAutomation	Accorde l'autorisation d'invoquer une automatisation d'écran	Écriture	screen-automation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDomains [autorisation uniquement]	Accorde l'autorisation de répertorier tous les domaines Amazon Honeycode et leur statut de vérification pour votre compte AWS	List			
ListGroups [autorisation uniquement]	Permet de répertorier tous les groupes d'une équipe Amazon Honeycode pour votre compte AWS	List			
ListTableColumns	Accorde l'autorisation de créer les colonnes dans une table.	Liste	table*		
ListTableRows	Accorde l'autorisation de répertorier les lignes dans une table.	Liste	table*		
ListTables	Accorde l'autorisation de répertorier les tables dans un classeur.	List	workbook*		
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises pour une ressource	Identification			
ListTeamAssociations [autorisation uniquement]	Accorde l'autorisation de répertorier toutes les associations d'équipe en attente et approuvées avec votre AWS compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTenants [autorisation uniquement]	Autorise à répertorier tous les locataires d'Amazon Honeycode pour votre compte AWS	List			
QueryTableRows	Accorde l'autorisation d'interroger les lignes d'une table à l'aide d'un filtre.	Lecture	table*		
RegisterDomainForVerification [autorisation uniquement]	Accorde l'autorisation de demander la vérification des domaines Amazon Honeycode pour votre compte AWS	Écrire			
RegisterGroups [autorisation uniquement]	Accorde l'autorisation d'ajouter des groupes à une équipe Amazon Honeycode pour votre compte AWS	Écrire			
RejectTeamAssociation [autorisation uniquement]	Autorise le rejet d'une demande d'association d'équipe pour votre AWS compte	Écrire			
RestartDomainVerification [autorisation uniquement]	Autorise le redémarrage de la vérification des domaines Amazon Honeycode pour votre compte AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartTableDataImportJob	Accorde l'autorisation de démarrer une tâche d'importation de données de table.	Écrire	table*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage			
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage			
UpdateTeam [autorisation uniquement]	Accorde l'autorisation de mettre à jour une équipe Amazon Honeycode pour votre compte AWS	Écrire			

Types de ressources définis par Amazon Honeycode

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workbook	`arn:${Partition}:honeycode:${Region}:${Account}:workbook:workbook/${WorkbookId}`	

Types de ressources	ARN	Clés de condition
table	`arn:${Partition}:honeycode:${Region}:${Account}:table:workbook/${WorkbookId}/table/${TableId}`	
screen	`arn:${Partition}:honeycode:${Region}:${Account}:screen:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}`	
screen-automation	`arn:${Partition}:honeycode:${Region}:${Account}:screen-automation:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}/automation/${AutomationId}`	

Clés de condition pour Amazon Honeycode

Honeycode ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS IAM Access Analyzer

AWS IAM Access Analyzer (préfixe de service :`access-analyzer`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IAM Access Analyzer
- Types de ressources définis par AWS IAM Access Analyzer
- Clés de condition pour AWS IAM Access Analyzer

Actions définies par AWS IAM Access Analyzer

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApplyArchiveRule	Accorde l'autorisation d'appliquer une règle d'archivage	Écriture	Analyzer*		
CancelPolicyGeneration	Accorde l'autorisation d'annuler une génération de politique.	Écrire			
CheckAccessNotGranted	Octroie l'autorisation de vérifier que l'accès spécifié n'est pas autorisé par une stratégie.	Lecture			
CheckNoNewAccess	Octroie l'autorisation de vérifier qu'aucun nouvel accès n'est autorisé par rapport à une stratégie existante.	Lecture			
CheckNoPublicAccess	Accorde l'autorisation de vérifier que l'accès public n'est	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	pas autorisé par une politique de ressources				
CreateAccessPreview	Accorde l'autorisation de créer un aperçu des accès pour l'analyseur spécifié	Écriture	Analyzer*		
CreateAnalyzer	Accorde l'autorisation de créer un analyseur	Écriture	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	Accorde l'autorisation de créer une règle d'archivage pour l'analyseur spécifié	Écriture	ArchiveRule*		
DeleteAnalyzer	Accorde l'autorisation de supprimer l'analyseur spécifié	Écriture	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteArchiveRule	Accorde l'autorisation de supprimer des règles d'archivage pour l'analyseur spécifié	Écrire	ArchiveRule*		
GenerateFindingRecommendation	Accorde l'autorisation de générer des étapes de recommandation pour résoudre une constatation	Écrire	Analyzer*		
GetAccessPreview	Accorde l'autorisation de récupérer des informations sur un aperçu des accès	Lecture	Analyzer*		
GetAnalyzedResource	Accorde l'autorisation de récupérer des informations sur une ressource analysée	Lecture	Analyzer*		
GetAnalyzer	Accorde l'autorisation de récupérer des informations sur des analyseurs	Lecture	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetArchiveRule	Accorde l'autorisation de récupérer des informations sur les règles d'archivage de l'analyseur spécifié	Lecture	ArchiveRule*		
GetFinding	Accorde l'autorisation de récupérer des résultats	Lecture	Analyzer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFindingRecommendation	Accorde l'autorisation de récupérer les étapes de recommandation pour résoudre une constatation	Lecture	Analyzer*		
GetFindingsStatistics	Octroie l'autorisation de récupérer des statistiques relatives à des résultats.	Lecture	Analyzer*		
GetGeneratedPolicy	Accorde l'autorisation de récupérer une politique qui a été générée à l'aide de StartPolicyGeneration	Lecture			
ListAccessPreviewFindings	Accorde l'autorisation de récupérer une liste de résultats à partir d'un aperçu des accès	Lecture	Analyzer*		
ListAccessPreviews	Accorde l'autorisation de récupérer une liste d'aperçus des accès	Liste	Analyzer*		
ListAnalyzedResources	Accorde l'autorisation de récupérer une liste des ressources qui ont été analysées	Lecture	Analyzer*		
ListAnalyzers	Accorde l'autorisation de récupérer une liste d'analyseurs	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListArchiveRules	Accorde l'autorisation de récupérer une liste de règles d'archivage à partir d'un analyseur	Liste	Analyzer*		
ListFindings	Accorde l'autorisation de récupérer une liste de résultats à partir d'un analyseur	Lecture	Analyzer*		
ListPolicyGenerations	Accorde l'autorisation de répertorier toutes les générations de politiques récemment démarrées.	Lecture			
ListTagsForResource	Accorde l'autorisation de récupérer une liste de balises appliquées à une ressource	Lecture	Analyzer		
StartPolicyGeneration	Accorde l'autorisation de démarrer une génération de politique.	Écriture			iam:PassRole
StartResourceScan	Accorde l'autorisation de lancer une analyse des stratégies appliquées à une ressource	Écriture	Analyzer*		
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource	Balisage	Analyzer		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	Analyzer		
				aws:TagKeys	
UpdateAnalyzer	Accorde l'autorisation de modifier la configuration d'un analyseur	Écrire	Analyzer*		
UpdateArchiveRule	Accorde l'autorisation de modifier une règle d'archivage	Écriture	ArchiveRule*		
UpdateFindings	Accorde l'autorisation de modifier des résultats	Écriture	Analyzer*		
ValidatePolicy	Accorde l'autorisation de valider une politique	Lecture			

Types de ressources définis par AWS IAM Access Analyzer

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}`	aws:ResourceTag/${TagKey}
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}/archive-rule/${RuleName}`	

Clés de condition pour AWS IAM Access Analyzer

AWS IAM Access Analyzer définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS IAM Identity Center

AWS IAM Identity Center (préfixe de service :`sso`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IAM Identity Center
- Types de ressources définis par AWS IAM Identity Center
- Clés de condition pour AWS IAM Identity Center

Actions définies par AWS IAM Identity Center

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddRegion	Accorde l'autorisation d'ajouter une région à une instance IAM Identity Center	Écrire	Instance*	sso:PrimaryRegion	identitystore:AddRegion kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateDirectory	Accorde l'autorisation de connecter un répertoire à utiliser par AWS IAM Identity Center	Écrire			ds:AuthorizeApplication identitystore:CreateIdentityStore kms:Decrypt
AssociateProfile	Accorde l'autorisation de créer une association entre un utilisateur de répertoire ou un groupe et un profil	Écrire			kms:Decrypt
AttachCustomerManagedPolicyReferenceToPermissionSet	Accorde l'autorisation d'attacher une référence de politique gérée par le client à un jeu d'autorisations	Gestion des autorisations	Instance* PermissionSet*	sso:PrimaryRegion sso:PrimaryRegion	kms:Decrypt
AttachManagedPolicyToPermissionSet	Accorde l'autorisation d'associer une politique AWS gérée à un ensemble d'autorisations	Gestion des autorisations	Instance* PermissionSet*	sso:PrimaryRegion sso:PrimaryRegion	kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAccountAssignment	Accorde l'autorisation d'attribuer l'accès à un principal pour un ensemble d'autorisations spécifié Compte AWS à l'aide d'un ensemble d'autorisations spécifié	Écrire	Account*		kms:Decrypt
			Instance*	sso:PrimaryRegion	
			PermissionSet*	sso:PrimaryRegion	
CreateApplication	Accorde l'autorisation de créer une application	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
			ApplicationProvider*		
			Instance*	sso:PrimaryRegion	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssignment	Octroie l'autorisation de créer une affectation d'application.	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApplicationInstance	Accorde l'autorisation d'ajouter une instance d'application à AWS IAM Identity Center	Écrire			kms:Decrypt
CreateApplicationInstanceCertificate	Accorde l'autorisation d'ajouter un nouveau certificat pour une instance d'application	Écrire			kms:Decrypt
CreateInstance	Octroie l'autorisation de créer une instance de centre d'identité.	Écrire	Instance*		iam:CreateServiceLinkedRole identitystore:CreateIdentityStore organizations:DescribeOrganization
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInstanceAccessControlAttributeConfiguration	Accorde l'autorisation d'activer l'instance pour ABAC et de spécifier les attributs	Écrire	Instance*	sso:PrimaryRegion	iam:AttachRolePolicy iam:CreateRole iam:DeleteRole iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:ListRolePolicies iam:PutRolePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:UpdateAssumeRolePolicy kms:Decrypt
CreateManagedApplicationInstance	Accorde l'autorisation d'ajouter une instance d'application gérée à AWS IAM Identity Center	Écrire			kms:Decrypt
CreatePermissionSet	Accorde l'autorisation de créer un jeu d'autorisations	Écriture	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Accorde l'autorisation de créer un profil pour une instance d'application	Écriture			kms:Decrypt
CreateTrust	Accorde l'autorisation de créer une approbation de fédération dans un compte cible	Écrire			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTrustedTokenIssuer	Octroie l'autorisation de créer un émetteur de jeton sécurisé pour une instance.	Écrire	Instance*	sso:PrimaryRegion	kms:Decrypt
			TrustedTokenIssuer*	sso:PrimaryRegion	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssignment	Accorde l'autorisation de supprimer l'accès d'un directeur à partir d'un ensemble d'autorisations spécifié Compte AWS à l'aide d'un ensemble d'autorisations spécifié	Écrire	Account*		kms:Decrypt
			Instance*	sso:PrimaryRegion	
			PermissionSet*	sso:PrimaryRegion	
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationAccessScope	Octroie l'autorisation de supprimer un champ d'accès à une application.	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				sso:ApplicationAccount	
DeleteApplicationAssignment	Octroie l'autorisation de supprimer une affectation d'application.	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationAuthenticationMethod	Octroie l'autorisation de supprimer une méthode d'authentification pour une application.	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationGrant	Octroie l'autorisation de supprimer une autorisation d'une application.	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationInstance	Accorde l'autorisation de supprimer l'instance de l'application	Écriture			kms:Decrypt
DeleteApplicationInstanceCertificate	Accorde l'autorisation pde our supprimer un certificat arrivé à expiration ou inactif de l'instance d'application	Écrire			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteInlinePolicyFromPermissionSet	Accorde l'autorisation de supprimer la politique en ligne d'un jeu d'autorisations spécifié	Écrire	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
DeleteInstance	Octroie l'autorisation de supprimer une instance de centre d'identité.	Écrire	Instance*	sso:PrimaryRegion	identitystore:DeleteIdentityStore
DeleteInstanceAccessControlAttributeConfiguration	Accorde l'autorisation de désactiver ABAC et de supprimer la liste des attributs de l'instance	Écriture	Instance*	sso:PrimaryRegion	kms:Decrypt
DeleteManagedApplicationInstance	Accorde l'autorisation de supprimer l'instance de l'application gérée	Écriture			kms:Decrypt
DeletePermissionSet	Accorde l'autorisation de supprimer un jeu d'autorisations	Écrire	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePermissionsBoundaryFromPermissionSet	Accorde l'autorisation de supprimer la limite d'autorisations d'un jeu d'autorisations	Gestion des autorisations	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
DeleteProfile	Accorde l'autorisation de supprimer le profil d'une instance d'application	Écrire			kms:Decrypt
DeleteTrustedTokenIssuer	Octroie l'autorisation de supprimer un émetteur de jeton sécurisé pour une instance.	Écrire	TrustedTokenIssuer*	sso:PrimaryRegion	kms:Decrypt
DescribeAccountAssignmentCreationStatus	Accorde l'autorisation de décrire le statut de la demande de création d'affectation	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt
DescribeAccountAssignmentDeletionStatus	Accorde l'autorisation de décrire le statut d'une demande de suppression d'affectation	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt
DescribeApplication	Octroie l'autorisation d'obtenir des informations sur une application.	Lecture	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeApplicationAssignment	Octroie l'autorisation de récupérer une affectation d'application.	Lecture	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
DescribeApplicationProvider	Octroie l'autorisation de décrire un fournisseur d'application.	Lecture	ApplicationProvider*		
DescribeInstance	Octroie l'autorisation d'obtenir des informations sur une instance de centre d'identité.	Lecture	Instance*	sso:PrimaryRegion	
DescribeInstanceAccessControlAttributeConfiguration	Accorde l'autorisation d'obtenir la liste des attributs utilisés par l'instance pour ABAC	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt
DescribePermissionSet	Accorde l'autorisation de décrire un jeu d'autorisations	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
DescribePermissionSetProvisioningStatus	Accorde l'autorisation de décrire l'état de la demande de provisionnement du jeu d'autorisations donnée	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRegion	Accorde l'autorisation de récupérer les détails de configuration pour une région d'instance IAM Identity Center spécifique	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt
DescribeRegisteredRegions	Accorde l'autorisation d'obtenir les régions dans lesquelles votre organisation a activé AWS IAM Identity Center	Lecture			
DescribeTrustedTokenIssuer	Octroie l'autorisation de décrire un émetteur de jeton sécurisé pour une instance.	Lecture	TrustedTokenIssuer*	sso:PrimaryRegion	kms:Decrypt
DetachCustomerManagedPolicyReferenceFromPermissionSet	Accorde l'autorisation de détacher une référence de politique gérée par le client d'un jeu d'autorisations	Gestion des autorisations	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
DetachManagedPolicyFromPermissionSet	Accorde l'autorisation de détacher la politique AWS gérée attachée de l'ensemble d'autorisations spécifié	Gestion des autorisations	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateDirectory	Accorde l'autorisation de dissocier un répertoire à utiliser par AWS IAM Identity Center	Écrire			ds:UnauthorizeApplication identitystore:DeleteIdentityStore kms:Decrypt
DisassociateProfile	Accorde l'autorisation de dissocier un utilisateur ou un groupe de répertoires d'un profil	Écrire			kms:Decrypt
GetApplicationAccessScope	Octroie l'autorisation d'obtenir un champ d'accès à une application.	Lecture	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	Octroie l'autorisation de lire des configurations d'affectation pour une application.	Lecture	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetApplicationAuthenticationMethod	Octroie l'autorisation d'obtenir une méthode d'authentification pour une application.	Lecture	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
GetApplicationGrant	Octroie l'autorisation d'obtenir des informations sur une autorisation associée à une application.	Lecture	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
GetApplicationInstance	Accorde l'autorisation de récupérer les détails d'une instance d'application	Lecture			kms:Decrypt
GetApplicationSessionConfiguration	Accorde l'autorisation d'obtenir la configuration de session pour une application	Lecture	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
GetApplicationTemplate	Accorde l'autorisation de récupérer les détails du modèle d'application	Lecture			
GetInlinePolicyForPermissionSet	Accorde l'autorisation d'obtenir la politique en ligne affectée au jeu d'autorisations	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			PermissionSet*	sso:PrimaryRegion	
GetManagedApplicationInstance	Accorde l'autorisation de récupérer les détails d'une instance d'application	Lecture			kms:Decrypt
GetMfaDeviceManagementForDirectory	Accorde l'autorisation de récupérer les paramètres de gestion des appareils MFA pour le répertoire	Lecture			kms:Decrypt
GetPermissionSet	Accorde l'autorisation de récupérer les détails d'un jeu d'autorisations	Lecture			kms:Decrypt
GetPermissionsBoundaryForPermissionSet	Accorde l'autorisation d'obtenir la limite d'autorisations pour un jeu d'autorisations	Lecture	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
GetProfile	Accorde l'autorisation de récupérer un profil pour une instance d'application	Lecture			kms:Decrypt
GetSSOStatus	Accorde l'autorisation de vérifier si AWS IAM Identity Center est activé	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSharedSsoConfiguration	Accorde l'autorisation de récupérer la configuration partagée pour l'instance SSO actuelle	Lecture			kms:Decrypt
GetSsoConfiguration	Accorde l'autorisation de récupérer la configuration de l'instance SSO actuelle	Lecture			kms:Decrypt
GetTrust	Accorde l'autorisation de récupérer l'approbation de fédération dans un compte cible	Lecture			kms:Decrypt
ImportApplicationInstanceServiceProviderMetadata	Accorde l'autorisation de mettre à jour l'instance d'application en chargeant un fichier de métadonnées SAML de l'application fourni par le fournisseur de service	Écrire			kms:Decrypt
ListAccountAssignmentCreationStatus	Accorde l'autorisation de répertorier le statut des demandes de création d' Compte AWS affectation pour une instance SSO spécifiée	List	Instance*	sso:PrimaryRegion	kms:Decrypt
ListAccountAssignmentDeletionStatus	Accorde l'autorisation de répertorier le statut des demandes de suppression d' Compte AWS affectation pour une instance SSO spécifiée	List	Instance*	sso:PrimaryRegion	kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAccountAssignments	Accorde l'autorisation de répertorier le destinataire du fichier spécifié Compte AWS avec l'ensemble d'autorisations spécifié	List	Account*		kms:Decrypt
			Instance*	sso:PrimaryRegion	
			PermissionSet*	sso:PrimaryRegion	
ListAccountAssignmentsForPrincipal	Octroie l'autorisation de répertorier les comptes affectés à un utilisateur ou à un groupe.	List	Instance*	sso:PrimaryRegion	kms:Decrypt
ListAccountsForProvisionedPermissionSet	Accorde l'autorisation de répertorier tous les AWS comptes pour lesquels l'ensemble d'autorisations spécifié est fourni	List	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
ListApplicationAccessScopes	Octroie l'autorisation de répertorier des champs d'accès à une application.	List	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
ListApplicationAssignments	Octroie l'autorisation de répertorier les affectations d'application.	List	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplicationAssignmentsForPrincipal	Octroie l'autorisation de répertorier les applications affectées à un utilisateur ou à un groupe.	List	Instance*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
ListApplicationAuthenticationMethods	Octroie l'autorisation de répertorier les méthodes d'authentification pour une application.	List	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
ListApplicationGrants	Octroie l'autorisation de répertorier les autorisations d'une application.	List	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	Accorde l'autorisation de récupérer tous les certificats pour une instance d'application donnée	Lecture			kms:Decrypt
ListApplicationInstances	Accorde l'autorisation de récupérer toutes les instances d'application	List			kms:Decrypt sso:GetApplicationInstance

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplicationProviders	Octroie l'autorisation de répertorier les fournisseurs d'applications.	List	ApplicationProvider*		
ListApplicationTemplates	Accorde l'autorisation de récupérer tous les modèles d'application pris en charge	List			sso:GetApplicationTemplate
ListApplications	Accorde l'autorisation pour récupérer toutes les applications associées à l'instance d'IAM Identity Center.	List			kms:Decrypt
ListCustomerManagedPolicyReferencesInPermissionSet	Accorde l'autorisation de répertorier les références de politiques gérées par le client qui sont attachées à un jeu d'autorisations spécifié	List	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
ListDirectoryAssociations	Accorde l'autorisation de récupérer les informations relatives à l'annuaire connecté à AWS IAM Identity Center	Lecture			kms:Decrypt
ListInstances	Accorde l'autorisation de répertorier les instances SSO auxquelles l'appelant a accès	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListManagedPoliciesInPermissionSet	Accorde l'autorisation de répertorier les politiques AWS gérées associées à un ensemble d'autorisations spécifié	List	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
ListPermissionSetProvisioningStatus	Accorde l'autorisation de répertorier le statut des demandes de provisionnement de jeu d'autorisations pour une instance SSO spécifiée	List	Instance*	sso:PrimaryRegion	kms:Decrypt
ListPermissionSets	Accorde l'autorisation de récupérer tous les jeux d'autorisations	List	Instance*	sso:PrimaryRegion	kms:Decrypt
ListPermissionSetsProvisionedToAccount	Accorde l'autorisation de répertorier tous les ensembles d'autorisations fournis à un Compte AWS	List	Account*		kms:Decrypt
			Instance*	sso:PrimaryRegion	
ListProfileAssociations	Accorde l'autorisation de récupérer l'utilisateur de répertoire ou le groupe associé au profil	Lecture			kms:Decrypt
ListProfiles	Accorde l'autorisation de récupérer tous les profils d'une instance d'application	List			kms:Decrypt sso:GetProfile

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRegions	Accorde l'autorisation de répertorier toutes les régions configurées pour une instance IAM Identity Center	List	Instance*	sso:PrimaryRegion	kms:Decrypt
ListTagsForResource	Accorde l'autorisation de répertorier les identifications qui sont attachées à la ressource spécifiée	Lecture	Application		kms:Decrypt
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
ListTrustedTokenIssuers	Octroie l'autorisation de répertorier les émetteurs de jetons sécurisés pour une instance.	List	Instance*	sso:PrimaryRegion	kms:Decrypt
ProvisionPermissionSet	Accorde l'autorisation de provisionner un jeu d'autorisations spécifié sur la cible spécifiée	Écrire	Account*		kms:Decrypt
			Instance*	sso:PrimaryRegion	
			PermissionSet*	sso:PrimaryRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutApplicationAccessScope	Accorde l'autorisation d'accéder à create/update une étendue d'accès à une application	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
PutApplicationAssignmentConfiguration	Accorde l'autorisation d'ajouter des configurations d'affectation à une application	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	Accorde l'autorisation d' create/update utiliser une méthode d'authentification à une application	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
PutApplicationGrant	Accorde l'autorisation d'octroyer create/update une subvention à une demande	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	
PutApplicationSessionConfiguration	Accorde l'autorisation de configurer une session pour une application	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				sso:ApplicationAccount	
PutInlinePolicyToPermissionSet	Accorde l'autorisation d'attacher une politique IAM en ligne à un jeu d'autorisations	Écrire	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
PutMfaDeviceManagementForDirectory	Accorde l'autorisation de placer les paramètres de gestion des appareils MFA pour le répertoire	Écrire			kms:Decrypt
PutPermissionsBoundaryToPermissionSet	Accorde l'autorisation d'ajouter la limite d'autorisations à un jeu d'autorisations	Gestion des autorisations	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
PutPermissionsPolicy	Accorde l'autorisation d'ajouter une politique à un jeu d'autorisations	Gestion des autorisations			kms:Decrypt
RemoveRegion	Accorde l'autorisation de supprimer une région d'une instance IAM Identity Center	Écrire	Instance*	sso:PrimaryRegion	identitystore:RemoveRegion kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchGroups	Accorde l'autorisation de rechercher des groupes dans le répertoire associé.	Lecture			ds:DescribeDirectories kms:Decrypt
SearchUsers	Accorde l'autorisation de rechercher des utilisateurs dans le répertoire associé.	Lecture			ds:DescribeDirectories kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartSSO	Accorde l'autorisation d'initialiser AWS IAM Identity Center	Écrire			kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	Accorde l'autorisation d'associer un jeu d'identifications à une ressource spécifiée	Identification	Application		kms:Decrypt
			Instance		
			PermissionSet		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			TrustedTokenIssuer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de dissocier un jeu d'identifications d'une ressource spécifiée	Identification	Application		kms:Decrypt
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écrire	Application*	sso:PrimaryRegion	kms:Decrypt
				sso:ApplicationAccount	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApplicationInstanceActiveCertificate	Accorde l'autorisation de définir un certificat en tant que certificat actif pour cette instance d'application	Écriture			kms:Decrypt
UpdateApplicationInstanceDisplayData	Accorde l'autorisation de mettre à jour les données d'affichage d'une instance d'application	Écriture			kms:Decrypt
UpdateApplicationInstanceResponseConfiguration	Accorde l'autorisation de mettre à jour la configuration de réponse de fédération pour l'instance d'application	Écriture			kms:Decrypt
UpdateApplicationInstanceResponseSchemaConfiguration	Accorde l'autorisation de mettre à jour la configuration du schéma de réponse de fédération pour l'instance d'application	Écriture			kms:Decrypt
UpdateApplicationInstanceSecurityConfiguration	Accorde l'autorisation de mettre à jour les détails de sécurité pour l'instance d'application	Écriture			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApplicationInstanceServiceProviderConfiguration	Accorde l'autorisation de mettre à jour la configuration relative au fournisseur de services pour l'instance d'application	Écriture			kms:Decrypt
UpdateApplicationInstanceStatus	Accorde l'autorisation de mettre à jour le statut d'une instance d'application	Écrire			kms:Decrypt
UpdateInstance	Octroie l'autorisation de mettre à jour une instance de centre d'identité.	Écrire	Instance*	sso:PrimaryRegion	identitystore:UpdateIdentityStore kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateInstanceAccessControlAttributeConfiguration	Accorde l'autorisation de mettre à jour les attributs à utiliser avec l'instance pour ABAC	Écriture	Instance*	sso:PrimaryRegion	kms:Decrypt
UpdateManagedApplicationInstanceStatus	Accorde l'autorisation de mettre à jour le statut d'une instance d'application gérée	Écrire			kms:Decrypt
UpdatePermissionSet	Accorde l'autorisation de mettre à jour le jeu d'autorisations	Gestion des autorisations	Instance*	sso:PrimaryRegion	kms:Decrypt
			PermissionSet*	sso:PrimaryRegion	
UpdateProfile	Accorde l'autorisation de mettre à jour le profil d'une instance d'application	Écriture			kms:Decrypt
UpdateSSOConfiguration	Accorde l'autorisation de mettre à jour la configuration de l'instance SSO actuelle	Écriture			kms:Decrypt
UpdateTrust	Accorde l'autorisation de mettre à jour l'approbation de fédération dans un compte cible	Écrire			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTrustedTokenIssuer	Octroie l'autorisation de mettre à jour un émetteur de jeton sécurisé pour une instance.	Écrire	TrustedTokenIssuer *	sso:PrimaryRegion	kms:Decrypt

Types de ressources définis par AWS IAM Identity Center

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	aws:ResourceTag/${TagKey} sso:PrimaryRegion
Account	`arn:${Partition}:sso:::account/${AccountId}`	
Instance	`arn:${Partition}:sso:::instance/${InstanceId}`	aws:ResourceTag/${TagKey} sso:PrimaryRegion
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
		sso:ApplicationAccount sso:PrimaryRegion
TrustedTokenIssuer	`arn:${Partition}:sso::${AccountId}:trustedTokenIssuer/${InstanceId}/${TrustedTokenIssuerId}`	aws:ResourceTag/${TagKey} sso:PrimaryRegion
ApplicationProvider	`arn:${Partition}:sso::aws:applicationProvider/${ApplicationProviderId}`	

Clés de condition pour AWS IAM Identity Center

AWS IAM Identity Center définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Clés de condition	Description	Type
identitycenter:ApplicationArn	Filtre l'accès par l'ARN de l'application IAM Identity Center	ARN
identitycenter:InstanceArn	Filtre l'accès par l'ARN de l'instance IAM Identity Center	ARN
sso:ApplicationAccount	Filtre l'accès en fonction du compte qui crée l'application. Cette clé de condition n'est pas prise en charge pour les applications SAML gérées par le client	String
sso:PrimaryRegion	Filtre l'accès par région principale de l'instance IAM Identity Center	String

Actions, ressources et clés de condition pour le répertoire AWS IAM Identity Center

AWS Le répertoire IAM Identity Center (préfixe de service :`sso-directory`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS répertoire IAM Identity Center
- Types de ressources définis par le AWS répertoire IAM Identity Center
- Clés de condition pour le AWS répertoire IAM Identity Center

Actions définies par le AWS répertoire IAM Identity Center

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddMemberToGroup	Accorde l'autorisation d'ajouter un membre à un groupe dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
CompleteVirtualMfaDeviceRegistration	Accorde l'autorisation de terminer le processus de création d'un périphérique MFA virtuel.	Écrire			
CompleteWebAuthnDeviceRegistration	Accorde l'autorisation de terminer le processus d'enregistrement d'un WebAuthn appareil	Écrire			
CreateAlias	Accorde l'autorisation de créer un alias pour le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			
CreateBearerToken	Accorde l'autorisation de créer un jeton porteur pour un locataire de provisionnement donné.	Écriture			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExternalIdPConfigurationForDirectory	Accorde l'autorisation de créer une configuration de fournisseur d'identité externe pour le répertoire.	Écrire			
CreateGroup	Accorde l'autorisation de créer un groupe dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
CreateProvisioningTenant	Accorde l'autorisation de créer un locataire de provisionnement pour un répertoire donné.	Écrire			kms:Decrypt
CreateUser	Accorde l'autorisation de créer un utilisateur dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
DeleteBearerToken	Accorde l'autorisation de supprimer un jeton porteur.	Écriture			kms:Decrypt
DeleteExternalIdPCertificate	Accorde l'autorisation de supprimer le certificat d'IdP externe donné.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteExternalIdPConfigurationForDirectory	Accorde l'autorisation de supprimer une configuration de fournisseur d'identité externe associée au répertoire.	Écrire			
DeleteGroup	Accorde l'autorisation de supprimer un groupe de l'annuaire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
DeleteMfaDeviceForUser	Accorde l'autorisation de supprimer un périphérique MFA par nom de périphérique pour un utilisateur donné.	Écriture			
DeleteProvisioningTenant	Accorde l'autorisation de supprimer le locataire de provisionnement.	Écrire			kms:Decrypt
DeleteUser	Accorde l'autorisation de supprimer un utilisateur de l'annuaire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
DescribeDirectory	Accorde l'autorisation de récupérer des informations sur le répertoire fourni par défaut par AWS IAM Identity Center	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGroup	Accorde l'autorisation d'interroger les données du groupe, à l'exclusion des membres de l'utilisateur et du groupe	Lecture			kms:Decrypt
DescribeGroups	Accorde l'autorisation de récupérer des informations sur les groupes à partir du répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
DescribeProvisioningTenant	Accorde l'autorisation de décrire le locataire de provisionnement	Lecture			kms:Decrypt
DescribeUser	Accorde l'autorisation de récupérer des informations sur un utilisateur à partir du répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
DescribeUserByUniqueAttribute	Accorde l'autorisation de décrire l'utilisateur avec un attribut unique valide représenté pour l'utilisateur	Lecture			kms:Decrypt
DescribeUsers	Accorde l'autorisation de récupérer des informations sur l'utilisateur à partir du répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableExternalIdPConfigurationForDirectory	Accorde l'autorisation de désactiver l'authentification des utilisateurs finaux à l'aide d'un fournisseur d'identité externe.	Écrire			
DisableUser	Accorde l'autorisation de désactiver un utilisateur dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
EnableExternalIdPConfigurationForDirectory	Accorde l'autorisation d'activer l'authentification des utilisateurs finaux avec un fournisseur d'identité externe.	Écrire			
EnableUser	Accorde l'autorisation d'activer l'utilisateur dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
GetAWSSPConfigurationForDirectory	Accorde l'autorisation de récupérer les configurations du fournisseur de services AWS IAM Identity Center pour l'annuaire	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGroupId	Accorde l'autorisation de récupérer les informations d'identification relatives au groupe dans le répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
GetUserId	Accorde l'autorisation de récupérer les informations d'identification relatives à l'utilisateur dans le répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
GetUserPoolInfo	(Obsolète) Accorde l'autorisation d'obtenir des informations UserPool	Lecture			
ImportExternalIdPCertificate	Accorde l'autorisation d'importer le certificat d'IdP utilisé pour vérifier des réponses IdP externes.	Écrire			
IsMemberInGroup	Accorde l'autorisation de vérifier si un membre fait partie du groupe dans le répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
IsMemberInGroups	Accorde l'autorisation de vérifier si un membre fait partie de plusieurs groupes dans le répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
ListBearerTokens	Accorde l'autorisation de répertorier les jetons porteurs pour un locataire de provisionnement donné.	Lecture			kms:Decrypt
ListExternalIdPCertificates	Accorde l'autorisation de répertorier les certificats d'IdP externes d'un répertoire d'un IdP donnés.	Lecture			
ListExternalIdPConfigurationsForDirectory	Accorde l'autorisation de répertorier toutes les configurations de fournisseur d'identité externe créées pour le répertoire.	Lecture			
ListGroups	Accorde l'autorisation de répertorier les groupes depuis le répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
ListGroupsForMember	Accorde l'autorisation de répertorier les groupes du membre cible	Lecture			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGroupsForUser	Accorde l'autorisation de répertorier les groupes d'un utilisateur à partir de l'annuaire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
ListMembersInGroup	Accorde l'autorisation de récupérer tous les membres qui font partie d'un groupe dans le répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt
ListMfaDevicesForUser	Accorde l'autorisation de répertorier tous les périphériques MFA actifs et leurs métadonnées de périphérique MFA pour un utilisateur.	Lecture			
ListProvisioningTenants	Accorde l'autorisation de répertorier les locataires de provisionnement pour un répertoire donné.	Lecture			kms:Decrypt
ListUsers	Accorde l'autorisation de répertorier les utilisateurs à partir du répertoire fourni par défaut par AWS IAM Identity Center	Lecture			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveMemberFromGroup	Accorde l'autorisation de supprimer un membre qui fait partie d'un groupe dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
SearchGroups	Accorde l'autorisation de rechercher des groupes dans le répertoire associé.	Lecture			kms:Decrypt
SearchUsers	Accorde l'autorisation de rechercher des utilisateurs dans le répertoire associé.	Lecture			kms:Decrypt
StartVirtualMfaDeviceRegistration	Accorde l'autorisation de commencer le processus de création d'un dispositif MFA virtuel.	Écrire			
StartWebAuthnDeviceRegistration	Autorise le lancement du processus d'enregistrement d'un WebAuthn appareil	Écrire			
UpdateExternalIdPConfigurationForDirectory	Accorde l'autorisation de mettre à jour une configuration de fournisseur d'identité externe associée au répertoire.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGroup	Accorde l'autorisation de mettre à jour les informations relatives à un groupe dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
UpdateGroupDisplayName	Accorde l'autorisation de mettre à jour le nom d'affichage du groupe/mettre à jour la réponse de nom d'affichage du groupe	Écriture			kms:Decrypt
UpdateMfaDeviceForUser	Accorde l'autorisation de mettre à jour les informations sur le dispositif MFA	Écrire			
UpdatePassword	Accorde l'autorisation de mettre à jour un mot de passe en envoyant un lien de réinitialisation du mot de passe par e-mail ou en générant un mot de passe à usage unique pour un utilisateur dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt
UpdateUser	Accorde l'autorisation de mettre à jour les informations utilisateur dans le répertoire fourni par défaut par AWS IAM Identity Center	Écrire			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateUserName	Accorde l'autorisation de mettre à jour le nom d'utilisateur de la réponse du nom d'utilisateur	Écriture			kms:Decrypt
VerifyEmail	Accorde l'autorisation de vérifier l'adresse e-mail d'un utilisateur.	Écrire			

Types de ressources définis par le AWS répertoire IAM Identity Center

AWS Le répertoire IAM Identity Center ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au répertoire AWS IAM Identity Center, spécifiez-le `"Resource": "*"` dans votre politique.

Clés de condition pour le AWS répertoire IAM Identity Center

Le répertoire IAM Identity Center ne contient aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le service AWS IAM Identity Center OIDC

AWS Le service IAM Identity Center OIDC (préfixe de service :`sso-oauth`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service AWS IAM Identity Center OIDC
- Types de ressources définis par le service AWS IAM Identity Center OIDC
- Clés de condition pour le AWS service IAM Identity Center OIDC

Actions définies par le service AWS IAM Identity Center OIDC

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTokenWithIAM	Accorde l'autorisation de créer et de renvoyer des jetons d'accès OAuth 2.0 et des jetons d'actualisation pour les applications clientes autorisées. Ces jetons peuvent contenir des étendues définies qui spécifient des autorisations telles que `read:profile` ou `write:data`	Écrire	Application*		kms:Decrypt
IntrospectTokenWithIAM	Accorde l'autorisation de valider et de récupérer des informations sur les jetons d'accès OAuth 2.0 actifs et	Écrire	Application*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]	les jetons d'actualisation, y compris leurs étendues et autorisations associées. Cette autorisation est utilisée uniquement par les applications AWS gérées et n'est pas documentée dans la référence d'API OIDC d'IAM Identity Center.				
RevokeTokenWithIAM [autorisation uniquement]	Accorde l'autorisation de révoquer les jetons d'accès OAuth 2.0 et d'actualiser les jetons, en les invalidant avant leur expiration normale. Cette autorisation est utilisée uniquement par les applications AWS gérées et n'est pas documentée dans la référence d'API OIDC d'IAM Identity Center.	Écrire	Application*		kms:Decrypt

Types de ressources définis par le service AWS IAM Identity Center OIDC

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	

Clés de condition pour le AWS service IAM Identity Center OIDC

Le service OIDC ne comporte aucune clé de contexte propre au service pouvant être utilisée dans l'élément `Condition` des instructions de politiques. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere (préfixe de service :`rolesanywhere`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Identity and Access Management Roles Anywhere
- Types de ressources définis par AWS Identity and Access Management Roles Anywhere
- Clés de condition pour AWS Identity and Access Management Roles Anywhere

Actions définies par AWS Identity and Access Management Roles Anywhere

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateProfile	Accorde l'autorisation de créer un profil	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateTrustAnchor	Accorde l'autorisation de créer un certificat approuvé (ou « trust anchor »)	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAttributeMapping	Accorde l'autorisation de supprimer une règle de mappage d'un profil	Écrire	profile*		
DeleteCrl	Accorde l'autorisation de supprimer une liste de révocation des certificats	Écrire	crl*		
DeleteProfile	Accorde l'autorisation de supprimer un profil.	Écrire	profile*		
DeleteTrustAnchor	Accorde l'autorisation de supprimer un certificat approuvé (ou « trust anchor »)	Écrire	trust-anchor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableCrl	Accorde l'autorisation de désactiver une liste de révocation des certificats	Écrire	crl*		
DisableProfile	Accorde l'autorisation de désactiver un profil	Écrire	profile*		
DisableTrustAnchor	Accorde l'autorisation de désactiver un certificat approuvé (ou « trust anchor »)	Écrire	trust-anchor*		
EnableCrl	Accorde l'autorisation d'activer une liste de révocation des certificats	Écrire	crl*		
EnableProfile	Accorde l'autorisation d'activer un profil	Écrire	profile*		iam:PassRole
EnableTrustAnchor	Accorde l'autorisation d'activer un certificat approuvé (ou « trust anchor »)	Écrire	trust-anchor*		
GetCrl	Accorde l'autorisation d'obtenir une liste de révocation des certificats	Lecture	crl*		
GetProfile	Accorde l'autorisation d'obtenir un profil	Lecture	profile*		
GetSubject	Accorde l'autorisation d'obtenir un objet	Lecture	subject*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTrustAnchor	Accorde l'autorisation d'obtenir un certificat approuvé (ou « trust anchor »)	Lecture	trust-anchor*		
ImportCrl	Accorde l'autorisation d'importer une liste de révocation des certificats	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	Accorde l'autorisation de répertorier des listes de révocation des certificats	List			
ListProfiles	Accorde l'autorisation de répertorier des profils	List			
ListSubjects	Accorde l'autorisation de répertorier des objets	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource.	List			
ListTrustAnchors	Accorde l'autorisation de répertorier des certificats approuvés (ou « trust anchor »)	List			
PutAttributeMapping	Accorde l'autorisation d'insérer une règle de mappage dans un profil	Écrire	profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutNotificationSettings	Accorde l'autorisation d'attacher des paramètres de notification à un point de confiance.	Écrire	trust-anchor*		
ResetNotificationSettings	Accorde l'autorisation de restaurer les paramètres de notification personnalisés à l'état par défaut défini par Rôles Anywhere IAM.	Écrire	trust-anchor*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	crl		
			profile		
			subject		
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	crl		
			profile		
			subject		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			trust-anchor		
				aws:TagKeys	
UpdateCrl	Accorde l'autorisation de mettre à jour une liste de révocation des certificats	Écrire	crl*		
UpdateProfile	Accorde l'autorisation de mettre à jour un profil	Écrire	profile*		iam:PassRole
UpdateTrustAnchor	Accorde l'autorisation de mettre à jour un certificat approuvé	Écrire	trust-anchor*		

Types de ressources définis par AWS Identity and Access Management Roles Anywhere

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
trust-anchor	arn:${Partition}:rolesanywhere:${Region}:${Account}:trust-anchor/${TrustAnchorId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:rolesanywhere:${Region}:${Account}:profile/${ProfileId}	aws:ResourceTag/${TagKey}
subject	arn:${Partition}:rolesanywhere:${Region}:${Account}:subject/${SubjectId}	aws:ResourceTag/${TagKey}
crl	arn:${Partition}:rolesanywhere:${Region}:${Account}:crl/${CrlId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Identity Store

AWS Identity Store (préfixe de service :`identitystore`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Identity Store
- Types de ressources définis par AWS Identity Store
- Clés de condition pour AWS Identity Store

Actions définies par AWS Identity Store

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddRegion	Accorde l'autorisation d'ajouter une région à un IdentityStore	Écrire			kms:Decrypt
CreateGroup	Accorde l'autorisation de créer un groupe dans le champ spécifié IdentityStore	Écrire	Identitystore*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
CreateGroupMembership	Accorde l'autorisation de créer un membre à un groupe dans le champ spécifié IdentityStore	Écrire	Group*		kms:Decrypt
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIdentityStore	Accorde l'autorisation de créer un nouveau IdentityStore dans un Compte AWS	Écrire			kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext
CreateUser	Accorde l'autorisation de créer un utilisateur dans le champ spécifié IdentityStore	Écrire	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers identitystore:ReservedUserId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteGroup	Accorde l'autorisation de supprimer un groupe dans le champ spécifié IdentityStore	Écrire	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion	
				identitystore:GroupExternalIdIssuers	
DeleteGroupMembership	Accorde l'autorisation de supprimer un membre qui fait partie d'un groupe dans le IdentityStore	Écrire	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
DeleteIdentityStore	Accorde l'autorisation de supprimer un IdentityStore	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteUser	Accorde l'autorisation de supprimer un utilisateur dans le champ spécifié IdentityStore	Écrire	Identitystore*		kms:Decrypt
			User*		
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
DescribeGroup	Accorde l'autorisation de récupérer des informations sur un groupe dans le champ spécifié IdentityStore	Lecture	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGroupMembership	Accorde l'autorisation de récupérer des informations sur un membre qui fait partie d'un groupe du groupe spécifié IdentityStore	Lecture	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
DescribeRegion	Accorde l'autorisation de récupérer les détails de configuration pour une IdentityStore région spécifique	Lecture		identitystore:PrimaryRegion	kms:Decrypt
DescribeUser	Accorde l'autorisation de récupérer des informations sur l'utilisateur dans le champ spécifié IdentityStore	Lecture	Identitystore*		kms:Decrypt
			User*		
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGroupId	Accorde l'autorisation de récupérer les informations d'identification du groupe dans le groupe spécifié IdentityStore	Lecture	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion	
GetGroupMembershipId	Accorde l'autorisation de récupérer les informations d'identification d'un membre qui fait partie d'un groupe du groupe spécifié IdentityStore	Lecture	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
GetUserId	Accorde l'autorisation de récupérer les informations d'identification de l'utilisateur dans le champ spécifié IdentityStore	Lecture	Identitystore*		kms:Decrypt
			User*		
				identitystore:PrimaryRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
IsMemberInGroups	Accorde l'autorisation de vérifier si un membre fait partie des groupes du groupe spécifié IdentityStore	Lecture	AllGroupMemberships*		kms:Decrypt
			Group*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
ListGroupMemberships	Accorde l'autorisation de récupérer tous les membres qui font partie d'un groupe dans le champ spécifié IdentityStore	List	AllGroupMemberships*		kms:Decrypt
			Group*		
			Identitystore*		
				identitystore:PrimaryRegion	
ListGroupMembershipsForMember	Accorde l'autorisation de répertorier les groupes du membre cible dans le champ spécifié IdentityStore	List	AllGroupMemberships*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
ListGroups	Accorde l'autorisation de rechercher des groupes dans le champ spécifié IdentityStore	List	AllGroups*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion	
				identitystore:GroupExternalIdIssuers	
ListRegions	Accorde l'autorisation de répertorier toutes les régions configurées pour un IdentityStore	List		identitystore:PrimaryRegion	kms:Decrypt
ListUsers	Accorde l'autorisation de rechercher des utilisateurs dans le champ spécifié IdentityStore	List	AllUsers*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Identitystore*		
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
RemoveRegion	Accorde l'autorisation de supprimer une région d'un IdentityStore	Écrire			kms:Decrypt
ReserveUser	Accorde l'autorisation de réserver un utilisateur en obtenant un UserID	Écrire	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion	
UpdateGroup	Accorde l'autorisation de mettre à jour les informations relatives à un groupe dans le champ spécifié IdentityStore	Écrire	Group*		kms:Decrypt
			Identitystore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
UpdateIdentityStore	Accorde l'autorisation de mettre à jour la configuration d'un IdentityStore	Écrire			kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext
UpdateUser	Accorde l'autorisation de mettre à jour les informations utilisateur dans le champ spécifié IdentityStore	Écrire	Identitystore* User*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	

Types de ressources définis par AWS Identity Store

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Identitystore	`arn:${Partition}:identitystore::${Account}:identitystore/${IdentityStoreId}`	
User	`arn:${Partition}:identitystore:::user/${UserId}`	
Group	`arn:${Partition}:identitystore:::group/${GroupId}`	

Types de ressources	ARN	Clés de condition
GroupMembership	arn:${Partition}:identitystore:::membership/${MembershipId}	
AllUsers	arn:${Partition}:identitystore:::user/*	
AllGroups	arn:${Partition}:identitystore:::group/*	
AllGroupMemberships	arn:${Partition}:identitystore:::membership/*	

Clés de condition pour AWS Identity Store

AWS Identity Store définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
identitystore:GroupExternalIdIssuers	Filtre l'accès par émetteur présent dans les ressources ExternalIds du groupe	ArrayOfARN
identitystore:IdentityStoreArn	Filtre l'accès par Identity Store (ARN)	ARN

Clés de condition	Description	Type
identitystore:PrimaryRegion	Filtre l'accès par région principale d'Identity Store	String
identitystore:ReservedUserId	Filtre l'accès en fonction d'un ID utilisateur préalablement réservé pour le CreateUser fonctionnement	String
identitystore:UserExternalIdIssuers	Filtre l'accès par émetteur présent dans ExternalIds les ressources utilisateur	ArrayOfARN
identitystore:UserId	Filtre l'accès par ID utilisateur Identity Store	String

Actions, ressources et clés de condition pour AWS Identity Store Auth

AWS Identity Store Auth (préfixe de service :`identitystore-auth`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Identity Store Auth
- Types de ressources définis par AWS Identity Store Auth
- Clés de condition pour AWS Identity Store Auth

Actions définies par AWS Identity Store Auth

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDeleteSession [autorisation uniquement]	Accorde l'autorisation de supprimer un lot de sessions spécifiées	Écrire			
BatchGetSession [autorisation uniquement]	Accorde l'autorisation de renvoyer les attributs de session pour un lot de sessions spécifiées	Lecture			
ListSessions [autorisation uniquement]	Accorde l'autorisation de récupérer une liste des sessions actives pour l'utilisateur spécifié	List			

Types de ressources définis par AWS Identity Store Auth

AWS Identity Store Auth ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Identity Store Auth, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Identity Store Auth

Identity Store Auth ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Identity Sync

AWS Identity Sync (préfixe de service :`identity-sync`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Identity Sync
- Types de ressources définis par AWS Identity Sync
- Clés de condition pour AWS Identity Sync

Actions définies par AWS Identity Sync

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison du journal vendu pour un profil de synchronisation	Gestion des autorisations	SyncProfileResource*		
CreateSyncFilter	Accorde l'autorisation de créer un filtre de synchronisation sur le profil de synchronisation	Écrire	SyncProfileResource*		
CreateSyncProfile	Accorde l'autorisation de créer un profil de synchronisation pour la source de l'identité	Écrire			ds:AuthorizeApplication
CreateSyncTarget	Accorde l'autorisation de créer une cible de synchronisation pour la source de l'identité	Écrire	SyncProfileResource*		
DeleteSyncFilter	Accorde l'autorisation de supprimer un filtre de synchronisation à partir du profil de synchronisation	Écrire	SyncProfileResource*		
DeleteSyncProfile	Accorde l'autorisation de supprimer un profil de synchronisation à partir de la source	Écrire	SyncProfileResource*		ds:UnauthorizeApplication
DeleteSyncTarget	Accorde l'autorisation de supprimer une cible de	Écrire	SyncProfileResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	synchronisation à partir de la source		SyncTargetResource*		
GetSyncProfile	Accorde l'autorisation de récupérer un profil de synchronisation à l'aide du nom du profil de synchronisation	Lecture	SyncProfileResource*		
GetSyncTarget	Accorde l'autorisation de récupérer une cible de synchronisation à partir du profil de synchronisation	Lecture	SyncProfileResource*		
			SyncTargetResource*		
ListSyncFilters	Accorde l'autorisation de répertorier les filtres de synchronisation à partir du profil de synchronisation	List	SyncProfileResource*		
StartSync	Accorde l'autorisation de démarrer un processus de synchronisation ou de continuer un processus de synchronisation précédemment mis en pause	Écrire	SyncProfileResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopSync	Accorde l'autorisation d'arrêter toutes les synchronisations planifiées dans le calendrier de synchronisation	Écrire	SyncProfileResource*		
UpdateSyncTarget	Accorde l'autorisation de mettre à jour une cible de synchronisation sur le profil de synchronisation	Écrire	SyncProfileResource*		
			SyncTargetResource*		

Types de ressources définis par AWS Identity Sync

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
SyncProfileResource	`arn:${Partition}:identity-sync:${Region}:${Account}:profile/${SyncProfileName}`	

Types de ressources	ARN	Clés de condition
SyncTargetResource	`arn:${Partition}:identity-sync:${Region}:${Account}:target/${SyncProfileName}/${SyncTargetName}`	

Clés de condition pour AWS Identity Sync

Identity Sync ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le service AWS Import Export Disk

AWS Le service Import Export Disk (préfixe de service :`importexport`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service AWS Import Export Disk
- Types de ressources définis par le service AWS Import Export Disk
- Clés de condition pour le service AWS Import Export Disk

Actions définies par le service AWS Import Export Disk

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelJob	Cette action annule une tâche spécifiée. Seul le propriétaire de la tâche peut l'annuler. L'action échoue si la tâche a déjà commencé ou est terminée.	Écriture			
CreateJob	Cette action démarre le processus de planification d'un chargement ou téléchargement de vos données.	Écrire			
GetShippingLabel	Cette action génère une étiquette d'expédition prépayée que vous utiliserez pour expédier votre appareil aux AWS fins de traitement.	Lecture			
GetStatus	Cette action renvoie des informations sur une tâche, notamment l'emplacement de la tâche dans le pipeline de traitement, l'état des résultats et la valeur de signature associée à la tâche.	Lecture			
ListJobs	Cette action renvoie les tâches associées au demandeur.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateJob	Vous pouvez utiliser cette action pour modifier les paramètres spécifiés dans le fichier manifeste d'origine en fournissant un nouveau fichier manifeste.	Écrire			

Types de ressources définis par le service AWS Import Export Disk

AWS Le service Import Export Disk ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Import Export Disk Service, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le service AWS Import Export Disk

Import/Export ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Inspector

Amazon Inspector (préfixe de service : `inspector`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Inspector
- Types de ressources définis par Amazon Inspector
- Clés de condition pour Amazon Inspector

Actions définies par Amazon Inspector

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddAttributesToFindings	Accorde l'autorisation d'attribuer des attributs (paires de clés et de valeurs) aux résultats qui sont spécifiés par les ARNs résultats	Écrire			
CreateAssessmentTarget	Accorde l'autorisation de créer une nouvelle cible d'évaluation à l'aide de l'ARN du groupe de ressources généré par CreateResourceGroup	Écrire			
CreateAssessmentTemplate	Accorde l'autorisation de créer un modèle d'évaluation pour l'objectif d'évaluation spécifié à partir de l'ARN de ce dernier	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExclusionsPreview	Accorde l'autorisation de lancer la génération d'un aperçu des exclusions pour le modèle d'évaluation spécifié	Écriture			
CreateResourceGroup	Accorde l'autorisation de créer un groupe de ressources à l'aide de l'ensemble spécifié des balises (paires de clés et de valeurs) qui sont utilisées pour sélectionner les instances EC2 à inclure dans un objectif d'évaluation Amazon Inspector	Écriture			
DeleteAssessmentRun	Accorde l'autorisation de supprimer l'exécution d'évaluation spécifiée à partir de l'ARN de celle-ci	Écriture			
DeleteAssessmentTarget	Accorde l'autorisation de supprimer l'objectif d'évaluation spécifié à partir de l'ARN de celui-ci	Écriture			
DeleteAssessmentTemplate	Accorde l'autorisation de supprimer le modèle d'évaluation spécifié à partir de l'ARN de celui-ci	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAssessmentRuns	Accorde l'autorisation de décrire les cycles d'évaluation spécifiés par le ou ARNs les cycles d'évaluation	Lecture			
DescribeAssessmentTargets	Accorde l'autorisation de décrire les cibles d'évaluation spécifiées par les ARNs cibles d'évaluation	Lecture			
DescribeAssessmentTemplates	Accorde l'autorisation de décrire les modèles d'évaluation spécifiés par les ARNs modèles d'évaluation	Lecture			
DescribeCrossAccountAccessRole	Accorde l'autorisation de décrire le rôle IAM qui permet à Amazon Inspector d'accéder à votre Compte AWS	Lecture			
DescribeExclusions	Accorde l'autorisation de décrire les exclusions spécifiées par les exclusions ARNs	Lecture			
DescribeFindings	Accorde l'autorisation de décrire les résultats spécifiés par ARNs les résultats	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeResourceGroups	Accorde l'autorisation de décrire les groupes de ressources spécifiés par les groupes ARNs de ressources	Lecture			
DescribeRulesPackages	Accorde l'autorisation de décrire les packages ARNs de règles spécifiés par le	Lecture			
GetAssessmentReport	Accorde l'autorisation de produire un rapport d'évaluation incluant les résultats détaillés et complets d'une exécution d'évaluation spécifiée	Lecture			
GetExclusionsPreview	Accorde l'autorisation de récupérer l'aperçu des exclusions (une liste d' ExclusionPreview objets) spécifié par le jeton d'aperçu	Lecture			
GetTelemetryMetadata	Accorde l'autorisation de récupérer des informations sur les données collectées pour l'exécution d'évaluation spécifiée	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAssessmentRunAgents	Accorde l'autorisation de répertorier les agents des séries d'évaluation spécifiés par les ARNs séries d'évaluation	List			
ListAssessmentRuns	Accorde l'autorisation de répertorier les séries d'évaluation correspondant aux modèles d'évaluation spécifiés par les ARNs modèles d'évaluation	List			
ListAssessmentTargets	Accorde l'autorisation de répertorier les cibles d'évaluation incluses dans ce ARNs Compte AWS	List			
ListAssessmentTemplates	Accorde l'autorisation de répertorier les modèles d'évaluation correspondant aux cibles d'évaluation spécifiées par les ARNs cibles d'évaluation	List			
ListEventSubscriptions	Accorde l'autorisation de répertorier tous les abonnements aux événements pour le modèle d'évaluation spécifié à partir de l'ARN de celui-ci	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListExclusions	Accorde l'autorisation de répertorier les exclusions générées par l'exécution d'évaluation	List			
ListFindings	Accorde l'autorisation de répertorier les résultats générés par les cycles d'évaluation spécifiés par les ARNs cycles d'évaluation	List			
ListRulesPackages	Accorde l'autorisation de répertorier tous les packages de règles Amazon Inspector disponibles	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises associées à un modèle d'évaluation	Lecture			
PreviewAgents	Accorde l'autorisation d'afficher un aperçu des agents installés sur les instances EC2 qui font partie de l'objectif d'évaluation spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterCrossAccountAccessRole	Accorde l'autorisation d'enregistrer le rôle IAM qu'Amazon Inspector utilise pour répertorier vos instances EC2 au début de l'exécution de l'évaluation ou lorsque vous lancez l'action PreviewAgents	Écrire			
RemoveAttributesFromFindings	Accorde l'autorisation de supprimer des attributs complets (paires de clés et de valeurs) ARNs des résultats spécifiés par les résultats lorsqu'un attribut avec la clé spécifiée existe	Écrire			
SetTagsForResource	Accorde l'autorisation de définir des balises (paires de clés et de valeurs) pour le modèle d'évaluation spécifié à partir de l'ARN de celui-ci	Balisage			
StartAssessmentRun	Accorde l'autorisation de lancer l'exécution d'évaluation spécifiée à partir de l'ARN du modèle d'évaluation	Écriture			
StopAssessmentRun	Accorde l'autorisation d'arrêter l'exécution d'évaluation spécifiée à partir de l'ARN de celle-ci	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SubscribeToEvent	Accorde l'autorisation d'activer le processus d'envoi de notifications Amazon Simple Notification Service (SNS) concernant un événement spécifié à une rubrique SNS spécifiée	Écriture			
UnsubscribeFromEvent	Accorde l'autorisation de désactiver le processus d'envoi de notifications Amazon Simple Notification Service (SNS) concernant un événement spécifié à une rubrique SNS spécifiée	Écriture			
UpdateAssessmentTarget	Accorde l'autorisation de mettre à jour l'objectif d'évaluation spécifié à partir de l'ARN de celui-ci	Écriture			

Types de ressources définis par Amazon Inspector

Amazon Inspector ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à Amazon Inspector, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Amazon Inspector

Inspector ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Inspector2

Amazon Inspector2 (préfixe de service : `inspector2`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Inspector2
- Types de ressources définis par Amazon Inspector2
- Clés de condition pour Amazon Inspector2

Actions définies par Amazon Inspector2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateMember	Accorde l'autorisation d'associer un compte à un compte administrateur Amazon Inspector	Écrire			
BatchAssociateCodeSecurityScanConfiguration	Accorde l'autorisation d'associer plusieurs référentiels de code à une configuration de scan de sécurité du code Amazon Inspector	Écrire			
BatchDisassociateCodeSecurityScanConfiguration	Accorde l'autorisation de dissocier plusieurs référentiels de code d'une configuration de scan de sécurité du code Amazon Inspector	Écrire			
BatchGetAccountStatus	Accorde l'autorisation de récupérer des informations sur les comptes Amazon Inspector pour un compte	Lecture			
BatchGetCodeSnippet	Octroie l'autorisation de récupérer des informations d'extrait de code relatives à un ou plusieurs résultats de vulnérabilité de code	Lecture			
BatchGetFindingDetails	Octroie l'autorisation pour un client d'obtenir des informati	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	ons détaillées sur les vulnérabilités à des fins de recherche.				
BatchGetFreeTrialInfo	Accorde l'autorisation de récupérer l'éligibilité à la période d'essai gratuite concernant les comptes Amazon Inspector d'un compte	Lecture			
BatchGetMemberEc2DeepInspectionStatus	Octroie à l'administrateur délégué l'autorisation de récupérer le statut d'inspection approfondie ec2 des comptes membres.	Lecture			
BatchUpdateMemberEc2DeepInspectionStatus	Octroie à l'administrateur délégué l'autorisation de mettre à jour le statut d'inspection approfondie ec2 des comptes membres associés.	Écrire			
CancelFindingsReport	Accorde l'autorisation d'annuler la génération d'un rapport sur les résultats	Écrire			
CancelSbomExport	Accorde l'autorisation d'annuler la génération d'un rapport SBOM	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCisScanConfiguration	Accorde l'autorisation de créer et de définir les paramètres d'une configuration de scan CIS	Écrire	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityIntegration	Accorde l'autorisation de créer une intégration de sécurité du code avec un fournisseur de référentiel de code source	Écrire	Code Security Integration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityScanConfiguration	Accorde l'autorisation de créer une configuration de scan pour l'analyse de sécurité du code	Écrire	Code Security Scan Configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	Accorde l'autorisation de créer et de définir les paramètres d'un filtre de résultats	Écrire	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsReport	Accorde l'autorisation de demander la génération d'un rapport sur les résultats	Écrire			
CreateSbomExport	Accorde l'autorisation de demander la génération d'un rapport SBOM	Écrire			
DeleteCisScanConfiguration	Accorde l'autorisation de supprimer une configuration de scan CIS	Écrire	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCodeSecurityIntegration	Accorde l'autorisation de supprimer une intégration de sécurité de code	Écrire	CodeSecurityIntegration*		
DeleteCodeSecurityScanConfiguration	Autorise la suppression d'une configuration de scan de sécurité par code	Écrire	CodeSecurityScanConfiguration*		
DeleteFilter	Accorde l'autorisation de supprimer un filtre de résultats	Écrire	Filter*		
DescribeOrganizationConfiguration	Accorde l'autorisation de récupérer des informations sur les paramètres de configuration d'Amazon Inspector pour une AWS organisation	Lecture			
Disable	Accorde l'autorisation de désactiver un compte Amazon Inspector	Écrire			
DisableDelegatedAdminAccount	Accorde l'autorisation de désactiver un compte en tant que compte administrateur Amazon Inspector délégué pour une AWS organisation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateMember	Accorde à un compte administrateur Amazon Inspector l'autorisation de se dissocier d'un compte membre Inspector	Écrire			
Enable	Accorde l'autorisation d'activer et de spécifier les paramètres de configuration d'un nouveau compte Amazon Inspector	Écrire			
EnableDelegatedAdminAccount	Accorde l'autorisation d'activer un compte en tant que compte administrateur Amazon Inspector délégué pour une AWS organisation	Écrire			
GetCisScanReport	Autorise la récupération d'un rapport contenant des informations sur les scans CIS terminés	Lecture			
GetCisScanResultDetails	Permet de récupérer des informations sur tous les détails relatifs à un scan CIS et à une ressource ciblée	List			
GetClustersForImage	Accorde l'autorisation d'obtenir des informations sur le cluster pour une image Amazon Ecr scannée en continu	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCodeSecurityIntegration	Accorde l'autorisation de récupérer des informations sur une intégration de sécurité du code	Lecture			
GetCodeSecurityScan	Accorde l'autorisation de récupérer des informations sur un scan de sécurité de code spécifique	Lecture			
GetCodeSecurityScanConfiguration	Accorde l'autorisation de récupérer des informations sur la configuration d'un scan de sécurité du code	Lecture			
GetConfiguration	Accorde l'autorisation de récupérer des informations sur les paramètres de configuration d'Amazon Inspector pour un Compte AWS	Lecture			
GetDelegatedAdminAccount	Accorde l'autorisation de récupérer des informations sur le compte administrateur Amazon Inspector pour un compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEc2DeepInspectionConfiguration	Octroie l'autorisation de récupérer la configuration d'inspection approfondie ec2 des comptes autonomes, des administrateurs délégués et des comptes membres.	Lecture			
GetEncryptionKey	Accorde l'autorisation de récupérer des informations sur la clé KMS utilisée pour chiffrer les extraits de code	Lecture			
GetFindingsReportStatus	Accorde l'autorisation de récupérer le statut d'un rapport sur les résultats demandé	Lecture			
GetMember	Accorde l'autorisation de récupérer des informations sur un compte associé à un compte administrateur Amazon Inspector	Lecture			
GetSbomExport	Accorde l'autorisation de récupérer un rapport SBOM demandé	Lecture			
ListAccountPermissions	Accorde l'autorisation de récupérer des autorisations de configuration des fonctionnalités associées à un compte Amazon Inspector au sein d'une organisation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCisScanConfigurations	Accorde l'autorisation de récupérer des informations sur toutes les configurations de scan CIS	List			
ListCisScanResultsAggregatedByChecks	Accorde l'autorisation de récupérer des informations sur toutes les vérifications relatives à un scan CIS	List			
ListCisScanResultsAggregatedByTargetResource	Permet de récupérer des informations sur toutes les ressources relatives à un scan CIS	List			
ListCisScans	Permet de récupérer des informations sur les scans CIS terminés	List			
ListCodeSecurityIntegrations	Permet de répertorier toutes les intégrations de sécurité du code dans votre compte	List			
ListCodeSecurityScanConfigurationAssociations	Accorde l'autorisation de répertorier les associations entre les référentiels de code et les configurations de scan de sécurité du code Amazon Inspector	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCodeSecurityScanConfigurations	Permet de répertorier toutes les configurations de scan de sécurité par code de votre compte	List			
ListCoverage	Accorde l'autorisation de récupérer les types de statistiques qu'Amazon Inspector peut générer pour les ressources surveillées par Inspector	List			
ListCoverageStatistics	Accorde l'autorisation de récupérer des informations statistiques et d'autres informations sur les ressources qu'Amazon Inspector surveille	List			
ListDelegatedAdminAccounts	Accorde l'autorisation de récupérer des informations sur le compte administrateur Amazon Inspector délégué à une AWS organisation	List			
ListFilters	Accorde l'autorisation de récupérer des informations sur tous les filtres de résultats	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFindingAggregations	Accorde l'autorisation de récupérer des données statistiques et d'autres informations sur les résultats d'Amazon Inspector	List			
ListFindings	Accorde l'autorisation de récupérer un sous-ensemble d'informations sur un ou plusieurs résultats	List			
ListMembers	Accorde l'autorisation de récupérer des informations sur les comptes membres Amazon Inspector associés à un compte administrateur Amazon Inspector	List			
ListTagsForResource	Accorde l'autorisation de récupérer les balises d'une ressource Amazon Inspector	Lecture			
ListUsageTotals	Accorde l'autorisation de récupérer des données d'utilisation agrégées pour un compte	List			
ResetEncryptionKey	Accorde l'autorisation à un client de réinitialiser l'utilisation d'une clé KMS appartenant à Amazon pour chiffrer des extraits de code	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchVulnerabilities	Accorde l'autorisation de répertorier les détails de la couverture d'Amazon Inspector pour une vulnérabilité spécifique	Lecture			
SendCisSessionHealth	Autorise l'envoi de l'état de santé du CIS pour un scan du CIS	Écrire			
SendCisSessionTelemetry	Accorde l'autorisation d'envoyer la télémétrie CIS pour un scan CIS	Écrire			
StartCisSession	Accorde l'autorisation de démarrer une session de scan CIS	Écrire			
StartCodeSecurityScan	Accorde l'autorisation de lancer une analyse de sécurité du code sur un référentiel spécifié	Écrire			
StopCisSession	Autorise l'arrêt d'une session de scan CIS	Écrire			
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour les balises d'une ressource Amazon Inspector	Identification	CIS Scan Configuration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Code Security Integration		
			Code Security Scan Configuration		
			Filter		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource Amazon Inspector	Identification	CIS Scan Configuration		
			Code Security Integration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Code Security Scan Configuration		
			Filter		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCisScanConfiguration	Accorde l'autorisation de mettre à jour les paramètres d'une configuration de scan CIS	Écrire	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateCodeSecurityIntegration	Autorise la mise à jour d'une intégration de sécurité de code existante	Écrire	Code Security Integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCodeSecurityScanConfiguration	Autorise la mise à jour d'une configuration d'analyse de sécurité du code existante	Écrire	Code Security Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateConfiguration	Accorde l'autorisation de mettre à jour les informations relatives aux paramètres de configuration d'Amazon Inspector pour un Compte AWS	Écrire			
UpdateEc2DeepInspectionConfiguration	Octroie l'autorisation de mettre à jour la configuration d'inspection approfondie ec2 à l'administrateur délégué et aux comptes membres et autonomes.	Écrire			
UpdateEncryptionKey	Accorde l'autorisation à un client d'utiliser une clé KMS pour chiffrer des extraits de code	Écrire			
UpdateFilter	Accorde l'autorisation de mettre à jour les paramètres d'un filtre de résultats	Écrire	Filter*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateOrgEc2DeepInspectionConfiguration	Octroie à l'administrateur délégué l'autorisation de mettre à jour la configuration d'inspection approfondie ec2 des comptes membres associés.	Écrire			
UpdateOrganizationConfiguration	Accorde l'autorisation de mettre à jour les paramètres de configuration d'Amazon Inspector pour une AWS organisation	Écrire			

Types de ressources définis par Amazon Inspector2

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Filter	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/filter/${FilterId}`	aws:ResourceTag/${TagKey}
Finding	`arn:${Partition}:inspector2:${Region}:${Account}:finding/${FindingId}`	
CIS Scan Configuration	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}`	aws:ResourceTag/${TagKey}
Code Security Scan Configuration	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/codesecurity-configuration/${CodeSecurityScanConfigurationId}`	aws:ResourceTag/${TagKey}
Code Security Integration	`arn:${Partition}:inspector2:${Region}:${Account}:codesecurity-integration/${CodeSecurityIntegrationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Inspector2

Amazon Inspector2 définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le canal de télémétrie Amazon Inspector2

Amazon Inspector2 Telemetry Channel (préfixe de service :`inspector2-telemetry`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le canal de télémétrie Amazon Inspector2
- Types de ressources définis par le canal de télémétrie Amazon Inspector2
- Clés de condition pour le canal de télémétrie Amazon Inspector2

Actions définies par le canal de télémétrie Amazon Inspector2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
NotifyHeartbeat	Accorde l'autorisation de notifier le rythme cardiaque pour une session de télémétrie active	Écrire			
SendTelemetry	Accorde l'autorisation d'envoyer des données télémétriques pour une session de télémétrie active	Écrire			
StartSession	Accorde l'autorisation de lancer une séance de télémétrie.	Écrire			
StopSession	Autorise l'arrêt d'une session de télémétrie	Écrire			

Types de ressources définis par le canal de télémétrie Amazon Inspector2

Amazon Inspector2 Telemetry Channel ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au canal de télémétrie Amazon Inspector2, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour le canal de télémétrie Amazon Inspector2

Inspector2Telemtry ne dispose d'aucune clé de contexte spécifique au service qui puisse être utilisée dans l'élément des déclarations de politique. `Condition` Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon InspectorScan

Amazon InspectorScan (préfixe de service :`inspector-scan`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon InspectorScan
- Types de ressources définis par Amazon InspectorScan
- Clés de condition pour Amazon InspectorScan

Actions définies par Amazon InspectorScan

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ScanSbom	Octroie l'autorisation d'analyser le SBOM fourni par le client et de renvoyer les vulnérabilités détectées en son sein.	Lecture			

Types de ressources définis par Amazon InspectorScan

Amazon InspectorScan ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon InspectorScan, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Amazon InspectorScan

InspectorScan ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Interactive Video Service

Amazon Interactive Video Service (préfixe de service : `ivs`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Interactive Video Service
- Types de ressources définis par Amazon Interactive Video Service
- Clés de condition pour Amazon Interactive Video Service

Actions définies par Amazon Interactive Video Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetChannel	Accorde l'autorisation d'obtenir plusieurs canaux simultanément par ARN de canal.	Lecture	Channel*		
BatchGetStreamKey	Accorde l'autorisation d'obtenir plusieurs clés de flux simultanément par ARN de clé de flux.	Lecture	StreamKey*		
BatchStartViewerSessionRevocation	Accorde l'autorisation de jouer simultanément StartViewerSessionRevocation sur plusieurs paires d'ARN et d'ID de téléspectateur	Écrire	Channel*		
CreateChannel	Accorde l'autorisation de créer un canal et une clé de flux associée.	Écrire	Channel*		
			StreamKey*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEncoderConfiguration	Octroie l'autorisation de créer une configuration d'encodeur.	Écrire	EncoderConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIngestConfiguration	Accorde l'autorisation de créer une nouvelle configuration d'ingestion	Écrire	Ingest-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateParticipantToken	Octroie l'autorisation de créer un jeton de participant	Écrire	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePlaybackRestrictionPolicy	Accorde l'autorisation de créer une politique de restriction de lecture	Écrire	Playback-Restriction-Policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRecordingConfiguration	Accorde l'autorisation de créer une configuration d'enregistrement.	Écrire	Recording-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStage	Octroie l'autorisation de créer une étape	Écrire	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStorageConfiguration	Octroie l'autorisation de créer une configuration de stockage.	Écrire	StorageConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamKey	Accorde l'autorisation de créer une clé de flux.	Écriture	Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Accorde l'autorisation de supprimer un canal et les clés de flux d'un canal.	Écrire	Channel*		
			Stream-Key*		
DeleteEncoderConfiguration	Octroie l'autorisation de supprimer une configuration d'encodeur pour l'ARN spécifié.	Écrire	Encoder-Configuration*		
DeleteIngestConfiguration	Accorde l'autorisation de supprimer une configuration d'ingestion pour l'ARN spécifié	Écrire	Ingest-Configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePlaybackKeyPair	Accorde l'autorisation de supprimer la paire de clés de lecture pour un ARN spécifié	Écrire	Playback-Key-Pair*		
DeletePlaybackRestrictionPolicy	Accorde l'autorisation de supprimer la politique de restriction de lecture pour un ARN spécifié	Écrire	Playback-Restriction-Policy*		
DeletePublicKey	Accorde l'autorisation de supprimer la clé publique pour l'ARN spécifié	Écrire	Public-Key*		
DeleteRecordingConfiguration	Accorde l'autorisation de supprimer une configuration d'enregistrement pour l'ARN spécifié.	Écrire	Recording-Configuration*		
DeleteStage	Octroie l'autorisation de supprimer l'étape d'un ARN spécifié	Écrire	Stage*		
DeleteStorageConfiguration	Octroie l'autorisation de supprimer une configuration de stockage pour l'ARN spécifié.	Écrire	Storage-Configuration*		
DeleteStreamKey	Accorde l'autorisation de supprimer la clé de flux pour un ARN spécifié	Écrire	Stream-Key*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisconnectParticipant	Octroie l'autorisation de déconnecter un participant de l'ARN d'étape spécifié	Écrire	Stage*		
GetChannel	Accorde l'autorisation d'obtenir la configuration de canal pour un ARN de canal spécifié	Lecture	Channel*		
GetComposition	Octroie l'autorisation d'obtenir la composition pour l'ARN spécifié.	Lecture	Composition*		
GetEncoderConfiguration	Octroie l'autorisation d'obtenir la configuration d'encodeur pour l'ARN spécifié.	Lecture	Encoder-Configuration*		
GetIngestConfiguration	Accorde l'autorisation d'obtenir la configuration d'ingestion pour l'ARN spécifié	Lecture	Ingest-Configuration*		
GetParticipant	Accorde l'autorisation d'obtenir des informations sur les participants pour un ARN d'étape, une session et un participant spécifiés	Lecture	Stage*		
GetPlaybackKeyPair	Accorde l'autorisation d'obtenir les informations des paires ce clés de lecture pour un ARN spécifié	Lecture	Playback-Key-Pair*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPlaybackRestrictionPolicy	Accorde l'autorisation d'obtenir la politique de restriction de lecture pour un ARN spécifié	Lecture	Playback-Restriction-Policy*		
GetPublicKey	Accorde l'autorisation d'obtenir la clé publique pour l'ARN spécifié	Lecture	Public-Key*		
GetRecordingConfiguration	Accorde l'autorisation d'obtenir la configuration d'enregistrement pour l'ARN spécifié.	Lecture	Recording-Configuration*		
GetStage	Octroie l'autorisation d'obtenir des informations d'étape pour un ARN spécifié	Lecture	Stage*		
GetStageSession	Accorde l'autorisation d'obtenir des informations de session d'étape pour un ARN d'étape et une session spécifiés	Lecture	Stage*		
GetStorageConfiguration	Octroie l'autorisation d'obtenir la configuration de stockage pour l'ARN spécifié.	Lecture	Storage-Configuration*		
GetStream	Accorde l'autorisation d'obtenir des informations sur le flux actif (en direct) sur un canal spécifié	Lecture	Channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStreamKey	Accorde l'autorisation d'obtenir des informations de clé de flux pour un ARN spécifié	Lecture	Stream-Key*		
GetStreamSession	Accorde l'autorisation d'obtenir des informations sur la session de flux sur un canal spécifié	Lecture	Channel*		
ImportPlaybackKeyPair	Accorde l'autorisation d'importer la clé publique.	Écrire	Playback-Key-Pair*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportPublicKey	Autorise l'importation d'une clé publique	Écrire	Public-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListChannels	Accorde l'autorisation d'obtenir des informations récapitulatives sur les canaux	List	Channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCompositions	Octroie l'autorisation d'obtenir des informations récapitulatives sur les compositions.	List	Encoder-Configuration		
			Stage		
ListEncoderConfigurations	Octroie l'autorisation d'obtenir des informations récapitulatives sur les configurations d'encodeur.	List			
ListIngestConfigurations	Accorde l'autorisation d'obtenir des informations récapitulatives sur les configurations d'ingestion	List			
ListParticipantEvents	Accorde l'autorisation de répertorier les événements des participants pour un ARN d'étape, une session et un participant spécifiés	List	Stage*		
ListParticipantReplicas	Accorde l'autorisation d'obtenir des informations récapitulatives sur les répliques des participants	List	Stage*		
ListParticipants	Accorde l'autorisation de répertorier les participants pour un ARN d'étape et une session spécifiés	List	Stage*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPlaybackKeyPairs	Accorde l'autorisation d'obtenir des informations récapitulatives sur les paires de clés de lecture	List	Playback-Key-Pair*		
ListPlaybackRestrictionPolicies	Accorde l'autorisation d'obtenir des informations récapitulatives sur les politiques de restriction de lecture	List			
ListPublicKeys	Accorde l'autorisation d'obtenir des informations récapitulatives sur les clés publiques	List			
ListRecordingConfigurations	Accorde l'autorisation d'obtenir des informations récapitulatives sur les configurations d'enregistrement.	List	Recording-Configuration*		
ListStageSessions	Accorde l'autorisation de répertorier les sessions d'étape pour un ARN d'étape spécifié	List	Stage*		
ListStages	Octroie l'autorisation d'obtenir des informations récapitulatives sur les étapes	List	Stage*		
ListStorageConfigurations	Octroie l'autorisation d'obtenir des informations récapitulatives sur les configurations de stockage.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStreamKeys	Accorde l'autorisation d'obtenir des informations récapitulatives sur les clés de flux	List	Channel*		
			Stream-Key*		
ListStreamSessions	Accorde l'autorisation d'obtenir des informations récapitulatives sur les sessions de flux sur un canal spécifié	List	Channel*		
ListStreams	Accorde l'autorisation d'obtenir des informations récapitulatives sur les flux en direct	Liste	Channel*		
ListTagsForResource	Accorde l'autorisation d'obtenir des informations sur les balises d'un ARN spécifié	Lecture	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutMetadata	Accorde l'autorisation d'insérer des métadonnées dans un flux RTMP pour un canal spécifié	Écrire	Channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartComposition	Octroie l'autorisation de démarrer une nouvelle composition.	Écrire	Encoder-Configuration*		
			Stage*		
			Channel		
			Storage-Configuration		
				aws:TagKeys aws:RequestTag/${TagKey}	
StartParticipantReplication	Accorde l'autorisation de démarrer la réplication d'un nouveau participant	Écrire	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartViewerSessionRevocation	Octroie l'autorisation de démarrer le processus de révocation de la session de l'utilisateur associée à un ARN de canal et à un ID d'utilisateur spécifiés.	Écrire	Channel*		
StopComposition	Octroie l'autorisation d'interrompre la composition pour l'ARN spécifié.	Écrire	Composition*		
StopParticipantReplication	Accorde l'autorisation d'arrêter la réplication des participants pour l'ARN spécifié	Écrire	Stage*		
StopStream	Accorde l'autorisation de déconnecter un streamer sur un canal spécifié	Écriture	Channel*		
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour des balises pour une ressource avec un ARN spécifié	Balisage	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des balises pour une ressource avec un ARN spécifié	Balisage	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys	
UpdateChannel	Accorde l'autorisation de mettre à jour la configuration d'un canal	Écrire	Channel*		
UpdateIngestConfiguration	Accorde l'autorisation de mettre à jour la configuration d'ingestion pour un ARN spécifié	Écrire	Ingest-Configuration*		
UpdatePlaybackRestrictionPolicy	Accorde l'autorisation de mettre à jour une politique de restriction de lecture pour un ARN spécifié	Écrire	Playback-Restriction-Policy*		
UpdateStage	Octroie l'autorisation de mettre à jour la configuration d'une étape	Écrire	Stage*		

Types de ressources définis par Amazon Interactive Video Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Channel	`arn:${Partition}:ivs:${Region}:${Account}:channel/${ResourceId}`	aws:ResourceTag/${TagKey}
Stream-Key	`arn:${Partition}:ivs:${Region}:${Account}:stream-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Key-Pair	`arn:${Partition}:ivs:${Region}:${Account}:playback-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Restriction-Policy	`arn:${Partition}:ivs:${Region}:${Account}:playback-restriction-policy/${ResourceId}`	aws:ResourceTag/${TagKey}
Recording-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:recording-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}
Stage	`arn:${Partition}:ivs:${Region}:${Account}:stage/${ResourceId}`	aws:ResourceTag/${TagKey}
Composition	`arn:${Partition}:ivs:${Region}:${Account}:composition/${ResourceId}`	aws:ResourceTag/${TagKey}
Encoder-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:encoder-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Storage-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:storage-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}
Public-Key	`arn:${Partition}:ivs:${Region}:${Account}:public-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Ingest-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:ingest-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Interactive Video Service

Amazon Interactive Video Service définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises associées à la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Interactive Video Service Chat

Amazon Interactive Video Service Chat (préfixe de service : `ivschat`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Interactive Video Service Chat
- Types de ressources définis par Amazon Interactive Video Service Chat
- Clés de condition pour Amazon Interactive Video Service Chat

Actions définies par Amazon Interactive Video Service Chat

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateChatToken	Accorde l'autorisation de créer un jeton crypté qui est utilisé pour établir une WebSocket connexion individuelle à une salle	Écrire	Room*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey}	
CreateLoggingConfiguration	Accorde l'autorisation de créer une configuration de journalisation qui permet aux clients d'enregistrer les messages de la salle	Écrire	Logging-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoom	Accorde l'autorisation de créer une salle permettant aux clients de se connecter et de transmettre des messages	Écrire	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLoggingConfiguration	Accorde l'autorisation de supprimer une configuration de journalisation pour un ARN de configuration de journalisation spécifié	Écrire	Logging-Configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteMessage	Accorde l'autorisation d'envoyer un événement à une salle spécifique qui demande aux clients de supprimer un message spécifique	Écrire	Room*		
DeleteRoom	Accorde l'autorisation de supprimer la salle pour un ARN de salle spécifié	Écrire	Room*		
DisconnectUser	Accorde l'autorisation de déconnecter toutes les connexions à l'aide d'un ID utilisateur spécifié d'une salle	Écrire	Room*		
GetLoggingConfiguration	Accorde l'autorisation d'obtenir une configuration de journalisation pour un ARN de configuration de journalisation spécifié	Lecture	Logging-Configuration*		
GetRoom	Accorde l'autorisation d'obtenir la configuration de la salle pour un ARN de salle spécifié	Lecture	Room*		
ListLoggingConfigurations	Accorde l'autorisation d'obtenir des informations récapitulatives sur les configurations de journalisation	List	Logging-Configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRooms	Accorde l'autorisation d'obtenir des informations récapitulatives sur les salles	List	Room*		
ListTagsForResource	Accorde l'autorisation d'obtenir des informations sur les balises d'un ARN spécifié	Lecture	Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
SendEvent	Accorde l'autorisation d'envoyer un événement à une salle	Écrire	Room*		
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour des balises pour une ressource avec un ARN spécifié	Balisage	Logging-Configuration		
			Room		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des balises pour une ressource avec un ARN spécifié	Identification	Logging-Configuration		
			Room		
				aws:TagKeys	
UpdateLoggingConfiguration	Accorde l'autorisation de mettre à jour une configuration de journalisation pour un ARN de configuration de journalisation spécifié	Écrire	Logging-Configuration*		
UpdateRoom	Accorde l'autorisation de mettre à jour la configuration de la salle pour un ARN de salle spécifié	Écrire	Room*		

Types de ressources définis par Amazon Interactive Video Service Chat

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Room	`arn:${Partition}:ivschat:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}
Logging-Configuration	`arn:${Partition}:ivschat:${Region}:${Account}:logging-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Interactive Video Service Chat

Amazon Interactive Video Service Chat définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises associées à la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour l' AWS interconnexion

AWS Interconnect (préfixe de service :`interconnect`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Interconnect
- Types de ressources définis par AWS Interconnect
- Clés de condition pour AWS Interconnect

Actions définies par AWS Interconnect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptConnectionProposal	Accorde l'autorisation d'accepter une proposition de connexion générée ailleurs	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Accorde l'autorisation de créer une connexion.	Écrire	connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConnection	Accorde l'autorisation de supprimer une connexion existante	Écrire	connection*		
DescribeConnectionProposal	Accorde l'autorisation de décrire une proposition de connexion	Lecture			
GetConnection	Accorde l'autorisation de décrire une connexion	Lecture	connection*		
GetEnvironment	Accorde l'autorisation de décrire un environnement	Lecture	environment*		
ListAttachPoints	Accorde l'autorisation de répertorier les points de rattachement disponibles	Lecture			
ListConnections	Accorde l'autorisation de répertorier les connexions	List			
ListEnvironments	Accorde l'autorisation de répertorier les environnements disponibles	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises sur une ressource	Lecture			
TagResource	Accorde l'autorisation d'appliquer des balises à une ressource	Identification	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	connection*		
				aws:TagKeys	
UpdateConnection	Autorise la mise à jour d'une connexion existante	Écrire	connection*		

Types de ressources définis par AWS Interconnect

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
connection	arn:${Partition}:interconnect:${Region}:${Account}:connection/${Id}	aws:ResourceTag/${TagKey}
environment	arn:${Partition}:interconnect:${Region}:${Account}:environment/${Id}	

Clés de condition pour AWS Interconnect

AWS L'interconnexion définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour le service de AWS facturation

AWS Le service de facturation (préfixe de service :`invoicing`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS service de facturation
- Types de ressources définis par le AWS service de facturation
- Clés de condition pour le AWS service de facturation

Actions définies par le AWS service de facturation

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetInvoiceProfile	Accorde l'autorisation d'obtenir les détails du profil de facturation d'un compte au sein de votre organisation	Lecture			
CreateInvoiceUnit	Accorde l'autorisation de créer une unité de facturation pour votre organisation	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateProcurementPortalPreference	Accorde l'autorisation de créer une préférence de portail d'approvisionnement	Écrire		aws:ResourceTag/${TagKey}	
DeleteInvoiceUnit	Autorise votre organisation à mettre à jour une unité de facturation	Écrire	invoice-unit*		
				aws:ResourceTag/${TagKey}	
DeleteProcurementPortalPreference	Autorise la suppression d'une préférence du portail d'approvisionnement	Écrire		aws:ResourceTag/${TagKey}	
GetInvoiceCorrection [autorisation uniquement]	Accorde l'autorisation d'obtenir une correction de facture	Lecture			
GetInvoiceEmailDeliveryPreferences [autorisation uniquement]	Accorde l'autorisation d'obtenir les préférences de livraison de la facture par e-mail	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInvoicePDF	Accorde l'autorisation d'obtenir une URL pré-signée du document de facture téléchargeable avec des documents supplémentaires	Lecture			
GetInvoiceUnit	Autorise votre organisation à obtenir des unités de facturation	Lecture	invoice-unit*		
GetProcurementPortalPreference	Accorde l'autorisation d'obtenir une préférence sur le portail d'approvisionnement	Lecture			
ListInvoiceCorrections [autorisation uniquement]	Accorde l'autorisation de répertorier les corrections de factures	List			
ListInvoiceSummaries	Accorde l'autorisation d'obtenir des informations récapitulatives sur les factures de votre compte ou d'un compte associé	Lecture			
ListInvoiceUnits	Autorise votre organisation à répertorier les unités de facturation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProcurementPortalPreferences	Accorde l'autorisation de répertorier les préférences du portail d'approvisionnement pour un compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	invoice-unit*		
				aws:ResourceTag/${TagKey}	
PutInvoiceEmailDeliveryPreferences [autorisation uniquement]	Accorde l'autorisation de définir les préférences de livraison de la facture par e-mail	Écrire			
PutProcurementPortalPreference	Autorise la mise à jour d'une préférence du portail d'approvisionnement	Écrire		aws:ResourceTag/${TagKey}	
StartInvoiceCorrection [autorisation uniquement]	Autorise le lancement de la correction des factures	Écrire			
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	invoice-unit*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	invoice-unit*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateInvoiceUnit	Autorise votre organisation à mettre à jour une unité de facturation	Écrire	invoice-unit*		
				aws:ResourceTag/${TagKey}	
UpdateProcurementPortalPreferenceStatus	Accorde l'autorisation de mettre à jour le statut d'une préférence de portail d'approvisionnement	Écrire		aws:ResourceTag/${TagKey}	

Types de ressources définis par le AWS service de facturation

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
invoice-unit	`arn:${Partition}:invoicing::${Account}:invoice-unit/${Identifier}`	aws:ResourceTag/${TagKey}
procurement-portal-preference	`arn:${Partition}:invoicing::${Account}:procurement-portal-preference/${Identifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour le AWS service de facturation

AWS Le service de facturation définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des étiquettes	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction de la présence d'étiquettes obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS IoT Analytics

AWS IoT Analytics (préfixe de service :`iotanalytics`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Analytics
- Types de ressources définis par AWS IoT Analytics
- Clés de condition pour AWS IoT Analytics

Actions définies par AWS IoT Analytics

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchPutMessage	Place un lot de messages dans le canal spécifié	Écrire	channel*		
CancelPipelineReprocessing	Annule le retraitement du pipeline spécifié	Écrire	pipeline*		
CreateChannel	Crée un canal	Écrire	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Crée un ensemble de données.	Écrire	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetContent	Génère le contenu du jeu de données spécifié (en exécutant les actions du jeu de données)	Écrire	dataset*		
CreateDatastore	Crée un entrepôt de données	Écrire	datastore*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Crée un pipeline	Écrire	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Supprime le canal spécifié	Écrire	channel*		
DeleteDataset	Supprime le jeu de données spécifié	Écrire	dataset*		
DeleteDatasetContent	Supprime le contenu du jeu de données spécifié	Écrire	dataset*		
DeleteDatastore	Supprime l'entrepôt de données spécifié	Écrire	datastore*		
DeletePipeline	Supprime le pipeline spécifié	Écrire	pipeline*		
DescribeChannel	Décrit le canal spécifié	Lecture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDataset	Décrit le jeu de données spécifié	Lecture	dataset*		
DescribeDatastore	Décrit l'entrepôt de données spécifié	Lecture	datastore*		
DescribeLoggingOptions	Décrit les options de journalisation du compte	Lecture			
DescribePipeline	Décrit le pipeline spécifié	Lecture	pipeline*		
GetDatasetContent	Obtient le contenu du jeu de données spécifié	Lecture	dataset*		
ListChannels	Répertorie les canaux du compte	List			
ListDatasetContents	Répertorie les informations relatives aux contenus des jeux de données qui ont été créés	List	dataset*		
ListDatasets	Répertorie les jeux de données du compte	List			
ListDatastores	Répertorie les entrepôts de données du compte	List			
ListPipelines	Répertorie les pipelines du compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Répertorie les identifications (métadonnées) que vous avez attribuées à la ressource	Lecture	channel		
			dataset		
			datastore		
			pipeline		
PutLoggingOptions	Place des options de journalisation pour le compte	Écrire			
RunPipelineActivity	Exécute l'activité de pipeline spécifiée	Lecture			
SampleChannelData	Fournit des exemples de données du canal spécifié	Lecture	channel*		
StartPipelineReprocessing	Démarre le retraitement du pipeline spécifié	Écrire	pipeline*		
TagResource	Ajoute ou modifie les balises de la ressource donnée. Les identifications sont des métadonnées qui peuvent être utilisées pour gérer une ressource.	Identification	channel		
			dataset		
			datastore		
			pipeline		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Supprime les identifications (métadonnées) données de la ressource	Identification	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateChannel	Met à jour le canal spécifié	Écrire	channel*		
UpdateDataset	Met à jour le jeu de données spécifié	Écrire	dataset*		
UpdateDatastore	Met à jour l'entrepôt de données spécifié	Écrire	datastore*		
UpdatePipeline	Met à jour le pipeline spécifié	Écrire	pipeline*		

Types de ressources définis par AWS IoT Analytics

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
channel	`arn:${Partition}:iotanalytics:${Region}:${Account}:channel/${ChannelName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
dataset	`arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/${DatasetName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
datastore	`arn:${Partition}:iotanalytics:${Region}:${Account}:datastore/${DatastoreName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:iotanalytics:${Region}:${Account}:pipeline/${PipelineName}`	aws:RequestTag/${TagKey} aws:TagKeys

Types de ressources	ARN	Clés de condition
		iotanalytics:ResourceTag/${TagKey}

Clés de condition pour AWS IoT Analytics

AWS IoT Analytics définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés de balise dans la demande	ArrayOfString
iotanalytics:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String

Actions, ressources et clés de condition pour AWS IoT Core Device Advisor

AWS IoT Core Device Advisor (préfixe de service :`iotdeviceadvisor`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Core Device Advisor
- Types de ressources définis par AWS IoT Core Device Advisor
- Clés de condition pour AWS IoT Core Device Advisor

Actions définies par AWS IoT Core Device Advisor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSuiteDefinition	Accorde l'autorisation de créer une définition de suite	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSuiteDefinition	Accorde l'autorisation de supprimer une définition de suite	Écrire	Suitedefinition*		
GetEndpoint	Accorde l'autorisation d'obtenir un point de terminaison Device Advisor	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSuiteDefinition	Accorde l'autorisation d'obtenir une définition de suite	Lecture	Suitedefinition*		
GetSuiteRun	Accorde l'autorisation d'obtenir l'exécution d'une suite	Lecture	Suiterun*		
GetSuiteRunReport	Accorde l'autorisation d'obtenir le rapport de qualification d'une exécution de suite	Lecture	Suiterun*		
ListSuiteDefinitions	Accorde l'autorisation de répertorier les définitions de suite	Liste			
ListSuiteRuns	Accorde l'autorisation de répertorier les exécutions de suite	Liste	Suitedefinition*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises (métadonnées) affectées à une ressource	Lecture	Suitedefinition		
			Suiterun		
StartSuiteRun	Accorde l'autorisation de lancer une exécution de suite	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
StopSuiteRun	Accorde l'autorisation d'arrêter une exécution de suite	Écriture	Suiterun*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter ou de modifier les balises de la ressource spécifiée. Les balises sont des métadonnées qui peuvent être utilisées pour gérer une ressource.	Balisage	Suitedefinition		
			Suiterun		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises données (métadonnées) d'une ressource	Balisage	Suitedefinition		
			Suiterun		
				aws:TagKeys	
UpdateSuiteDefinition	Accorde l'autorisation de mettre à jour une définition de suite	Écrire	Suitedefinition*		

Types de ressources définis par AWS IoT Core Device Advisor

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Suitedefinition	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suitedefinition/${SuiteDefinitionId}`	aws:ResourceTag/${TagKey}
Suiterun	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suiterun/${SuiteDefinitionId}/${SuiteRunId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS IoT Core Device Advisor

AWS IoT Core Device Advisor définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le testeur d'appareils AWS IoT

AWS IoT Device Tester (préfixe de service :`iot-device-tester`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Device Tester
- Types de ressources définis par AWS IoT Device Tester
- Clés de condition pour le testeur d'appareils AWS IoT

Actions définies par AWS IoT Device Tester

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CheckVersion	Accorde l'autorisation à IoT Device Tester de vérifier si un ensemble donné de produit, une suite de tests et une version de testeur d'appareils sont compatibles	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DownloadTestSuite	Accorde l'autorisation à IoT Device Tester de télécharger des versions compatibles de la suite de tests	Lecture			
LatestIdt	Accorde l'autorisation à IoT Device Tester d'obtenir des informations sur la dernière version du testeur d'appareils disponible	Lecture			
SendMetrics	Accorde les autorisations à IoT Device Tester d'envoyer des métriques d'utilisation en votre nom	Écrire			
SupportedVersion	Accorde l'autorisation à IoT Device Tester d'obtenir la liste des produits pris en charge et des versions de la suite de tests	Lecture			

Types de ressources définis par AWS IoT Device Tester

AWS IoT Device Tester ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS IoT Device Tester, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le testeur d'appareils AWS IoT

IoT Device Tester ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour la liste des clés de contexte globales disponibles pour tous les services, voir Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS IoT Events

AWS IoT Events (préfixe de service :`iotevents`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Events
- Types de ressources définis par AWS IoT Events
- Clés de condition pour AWS IoT Events

Actions définies par AWS IoT Events

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les

ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchAcknowledgeAlarm	Accorde l'autorisation d'envoyer une ou plusieurs demandes d'accusé de réception à AWS IoT Events	Écrire	alarmModel*		
BatchDeleteDetector	Autorise la suppression d'une instance de détecteur dans le système AWS IoT Events	Écrire	detectorModel*		
BatchDisableAlarm	Accorde l'autorisation de désactiver une ou plusieurs instances d'alarme	Écriture	alarmModel*		
BatchEnableAlarm	Accorde l'autorisation d'activer une ou plusieurs instances d'alarme	Écrire	alarmModel*		
BatchPutMessage	Accorde l'autorisation d'envoyer un ensemble de messages au système AWS IoT Events	Écrire	input*		
BatchResetAlarm	Accorde l'autorisation de réinitialiser une ou plusieurs instances d'alarme	Écriture	alarmModel*		
BatchSnoozeAlarm	Accorde l'autorisation de modifier une ou plusieurs instances d'alarme en mode Snooze	Écrire	alarmModel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdateDetector	Autorise la mise à jour d'une instance de détecteur dans le système AWS IoT Events	Écrire	detectorModel*		
CreateAlarmModel	Autorise la création d'un modèle d'alarme pour surveiller un attribut d'entrée AWS IoT Events ou une propriété d'un SiteWise actif AWS IoT	Écrire	alarmModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorModel	Autorise la création d'un modèle de détecteur pour surveiller un attribut d'entrée AWS IoT Events	Écrire	detectorModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Accorde l'autorisation de créer une entrée dans IotEvents	Écrire	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAlarmModel	Accorde l'autorisation de supprimer un modèle d'alarme	Écriture	alarmModel*		
DeleteDetectorModel	Accorde l'autorisation de supprimer un modèle de détecteur	Écriture	detectorModel*		
DeleteInput	Accorde l'autorisation de supprimer une entrée.	Écriture	input*		
DescribeAlarm	Accorde l'autorisation de récupérer les informations sur une instance d'alarme	Lecture	alarmModel*		
DescribeAlarmModel	Accorde l'autorisation de récupérer les informations sur un modèle d'alarme	Lecture	alarmModel*		
DescribeDetector	Accorde l'autorisation de récupérer les informations sur une instance de détecteur	Lecture	detectorModel*		
DescribeDetectorModel	Accorde l'autorisation de récupérer les informations sur un modèle de détecteur	Lecture	detectorModel*		
DescribeDetectorModelAnalysis	Accorde l'autorisation de récupérer les informations sur l'analyse d'un modèle de détecteur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeInput	Accorde l'autorisation de récupérer les informations sur une entrée	Lecture	input*		
DescribeLoggingOptions	Accorde l'autorisation de récupérer les paramètres actuels des options de journalisation des événements AWS IoT	Lecture			
GetDetectorModelAnalysisResults	Accorde l'autorisation de récupérer les résultats de l'analyse du modèle de détecteur	Lecture			
ListAlarmModelVersions	Accorde l'autorisation de répertorier toutes les versions d'un modèle d'alarme	Liste	alarmModel*		
ListAlarmModels	Accorde l'autorisation de répertorier les modèles d'alarmes que vous avez créés	Liste			
ListAlarms	Accorde l'autorisation de récupérer les informations sur toutes les instances d'alarme par alarmModel	Liste	alarmModel*		
ListDetectorModelVersions	Accorde l'autorisation de récupérer toutes les versions d'un modèle de détecteur	Liste	detectorModel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDetectorModels	Accorde l'autorisation de récupérer les modèles de détecteur que vous avez créés	Liste			
ListDetectors	Accorde l'autorisation de récupérer les informations sur toutes les instances de détecteur par detectormodel	Liste	detectorModel*		
ListInputRoutings	Accorde l'autorisation de répertorier un ou plusieurs routages d'entrée	Liste			
ListInputs	Accorde l'autorisation de répertorier les entrées que vous avez créées	Liste			
ListTagsForResource	Accorde l'autorisation de récupérer les identifications (métadonnées) que vous avez affectées à la ressource	Lecture	alarmModel		
			detectorModel		
			input		
PutLoggingOptions	Accorde l'autorisation de définir ou de mettre à jour les options de journalisation des événements AWS IoT	Écrire			
StartDetectorModelAnalysis	Accorde l'autorisation de démarrer l'analyse du modèle de détecteur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter ou de modifier les balises d'une ressource donnée. Les balises sont des métadonnées qui peuvent être utilisées pour gérer une ressource.	Balisage	alarmModel		
			detectorModel		
			input		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les identifications données (métadonnées) de la ressource	Balisage	alarmModel		
			detectorModel		
			input		
				aws:TagKeys	
UpdateAlarmModel	Accorde l'autorisation de mettre à jour un modèle d'alarme	Écriture	alarmModel*		
UpdateDetectorModel	Accorde l'autorisation de mettre à jour un modèle de détecteur	Écriture	detectorModel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateInput	Accorde l'autorisation de mettre à jour une entrée.	Écriture	input*		
UpdateInputRouting	Accorde l'autorisation de mettre à jour le routage d'entrée	Écrire	input*		

Types de ressources définis par AWS IoT Events

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
detectorModel	`arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/${DetectorModelName}`	aws:ResourceTag/${TagKey}
alarmModel	`arn:${Partition}:iotevents:${Region}:${Account}:alarmModel/${AlarmModelName}`	aws:ResourceTag/${TagKey}
input	`arn:${Partition}:iotevents:${Region}:${Account}:input/${InputName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS IoT Events

AWS IoT Events définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource	Chaîne
aws:TagKeys	Filtrer les actions en fonction des clés de balise dans la demande	ArrayOfString
iotevents:keyValue	Filtre l'accès en fonction de l'InstanceId (clé-valeur) du message	String

Actions, ressources et clés de condition pour AWS IoT Fleet Hub pour la gestion des appareils

AWS IoT Fleet Hub for Device Management (préfixe de service :`iotfleethub`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Fleet Hub pour la gestion des appareils
- Types de ressources définis par AWS IoT Fleet Hub pour la gestion des appareils
- Clés de condition pour AWS IoT Fleet Hub pour la gestion des appareils

Actions définies par AWS IoT Fleet Hub pour la gestion des appareils

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApplication	Accorde l'autorisation de créer une application	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
DeleteApplication	Accorde l'autorisation de supprimer une application	Écriture	application*		sso:DeleteManagedApplicationInstance
DescribeApplication	Accorde l'autorisation de décrire une application	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplications	Accorde l'autorisation de répertorier toutes les applications	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises pour une ressource	Lecture	application		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	application		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	application		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écrire	application*		

Types de ressources définis par AWS IoT Fleet Hub pour la gestion des appareils

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:iotfleethub:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS IoT Fleet Hub pour la gestion des appareils

AWS IoT Fleet Hub for Device Management définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource	Chaîne
aws:TagKeys	Filtrer les actions en fonction des clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS l'IoT FleetWise

AWS L'IoT FleetWise (préfixe de service :`iotfleetwise`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l' AWS IoT FleetWise
- Types de ressources définis par AWS l'IoT FleetWise
- Clés de condition pour AWS l'IoT FleetWise

Actions définies par l' AWS IoT FleetWise

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateVehicleFleet	Accorde l'autorisation d'associer le véhicule donné à une flotte	Écrire	fleet*		
			vehicle*		
CreateCampaign	Accorde l'autorisation de créer une campagne	Écrire	campaign*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			fleet*		
			signalcatalog*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys iotfleetwise:DestinationArn	
CreateDecoderManifest	Accorde l'autorisation de créer un manifeste de décodeur pour un modèle existant	Écrire	decodermanifest*		
			modelmanifest*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFleet	Accorde l'autorisation de créer une flotte	Écrire	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelManifest	Accorde l'autorisation de créer une définition de modèle de manifeste	Écrire	modelmanifest*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalCatalog	Accorde l'autorisation de créer un catalogue de signaux	Écrire	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateStateTemplate	Accorde l'autorisation de créer un modèle d'état	Écrire	signalcatalog*		
			statetemplate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVehicle	Accorde l'autorisation de créer un véhicule	Écrire	decodermanifest*		iot:CreateThing iot:DescribeThing
			modelmanifest*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCampaign	Accorde l'autorisation de supprimer une campagne	Écrire	campaign*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDecoderManifest	Accorde l'autorisation de supprimer le manifeste de décodeur donné	Écrire	decodermanifest*		
DeleteFleet	Accorde l'autorisation de supprimer une flotte	Écrire	fleet*		
DeleteModelManifest	Accorde l'autorisation de supprimer le modèle de manifeste donné	Écrire	modelmanifest*		
DeleteSignalCatalog	Accorde l'autorisation de supprimer un catalogue de signaux spécifique	Écrire	signalcatalog*		
DeleteStateTemplate	Accorde l'autorisation de supprimer un modèle d'état	Écrire	statetemplate*		
DeleteVehicle	Accorde l'autorisation de supprimer un véhicule	Écrire	vehicle*		
DisassociateVehicleFleet	Accorde l'autorisation de dissocier un véhicule d'une flotte existante	Écrire	fleet*		
			vehicle*		
GenerateCommandPayload [autorisation uniquement]	Accorde l'autorisation de générer la charge utile pour exécuter une commande sur un véhicule	Gestion des autorisations	vehicle*		
			statetemplate		
				iotfleetwise:Signals	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCampaign	Accorde l'autorisation d'obtenir des informations récapitulatives pour une campagne donnée	Lecture	campaign*		
GetDecoderManifest	Accorde l'autorisation d'obtenir des informations récapitulatives pour une définition de manifeste de décodeur donnée	Lecture	decodermanifest*		
GetEncryptionConfiguration	Accorde l'autorisation d'obtenir l'état de chiffrement basé sur le KMS pour Compte AWS	Lecture			
GetFleet	Accorde l'autorisation d'obtenir des informations récapitulatives pour une flotte	Lecture	fleet*		
GetLoggingOptions	Accorde l'autorisation d'obtenir les options de journalisation pour Compte AWS	Lecture			
GetModelManifest	Accorde l'autorisation d'obtenir des informations récapitulatives pour une définition de modèle de manifeste donnée	Lecture	modelmanifest*		
GetRegisterAccountStatus	Accorde l'autorisation d'obtenir le statut d'enregistrement du compte auprès de l'IoT FleetWise	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSignalCatalog	Accorde l'autorisation d'obtenir des informations récapitulatives pour un catalogue de signaux spécifique	Lecture	signalcatalog*		
GetStateTemplate	Accorde l'autorisation d'obtenir des informations récapitulatives pour un modèle d'état donné	Lecture	statetemplate*		
GetVehicle	Accorde l'autorisation d'obtenir des informations récapitulatives pour un véhicule	Lecture	vehicle*		
GetVehicleStatus	Accorde l'autorisation d'obtenir l'état des campagnes exécutées sur un véhicule spécifique	Lecture	vehicle*		
ImportDecoderManifest	Accorde l'autorisation d'importer un manifeste de décodeur existant	Écrire	decodermanifest*		
ImportSignalCatalog	Accorde l'autorisation de créer un catalogue de signaux en important des définitions existantes	Écrire	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCampaigns	Accorde l'autorisation de répertorier des campagnes	Lecture			
ListDecoderManifestNetworkInterfaces	Accorde l'autorisation de répertorier les interfaces réseau associées au manifeste de décodeur existant	List	decodermanifest*		
ListDecoderManifestSignals	Accorde l'autorisation de répertorier les signaux du manifeste de décodeur.	List	decodermanifest*		
ListDecoderManifests	Accorde l'autorisation de répertorier tous les manifestes de décodeur, avec un filtre facultatif sur le modèle de manifeste	Lecture			
ListFleets	Accorde l'autorisation de répertorier toutes les flottes	Lecture			
ListFleetsForVehicle	Accorde l'autorisation de répertorier toutes les flottes auxquelles le véhicule est associé	Lecture	vehicle*		
ListModelManifestNodes	Accorde l'autorisation de répertorier tous les nœuds pour le modèle de manifeste donné.	List	modelmanifest*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListModelManifests	Accorde l'autorisation de répertorier tous les modèles de manifeste, avec un filtre facultatif sur le catalogue de signaux	Lecture			
ListSignalCatalogNodes	Accorde l'autorisation de répertorier tous les nœuds d'un catalogue de signaux donné	Lecture	signalcatalog*		
ListSignalCatalogs	Accorde l'autorisation de répertorier tous les catalogues de signaux	Lecture			
ListStateTemplates	Accorde l'autorisation de répertorier les modèles d'état	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			vehicle		
ListVehicles	Accorde l'autorisation de répertorier tous les véhicules, avec un filtre facultatif sur le modèle de manifeste	Lecture			
ListVehiclesInFleet	Accorde l'autorisation de répertorier les véhicules d'une flotte donnée	Lecture	fleet*		
PutEncryptionConfiguration	Accorde l'autorisation d'activer ou de désactiver le chiffrement basé sur KMS pour Compte AWS	Écrire			
PutLoggingOptions	Accorde l'autorisation de définir les options de journalisation pour Compte AWS	Écrire			
RegisterAccount	Donne l'autorisation d' Compte AWS enregistrer un IoT FleetWise	Écrire			iam:PassRole
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	campaign		
			decodermanifest		
			fleet		
			modelmanifest		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			signalcatalog		
			statetemplate		
			vehicle		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateCampaign	Accorde l'autorisation de mettre à jour la campagne donnée	Écrire	campaign*		
UpdateDecoderManifest	Accorde l'autorisation de mettre à jour une définition de manifeste de décodeur	Écrire	decodermanifest*		
UpdateFleet	Accorde l'autorisation de mettre à jour la flotte	Écrire	fleet*		
UpdateModelManifest	Accorde l'autorisation de mettre à jour la définition du modèle de manifeste donnée	Écrire	modelmanifest*		
UpdateSignalCatalog	Accorde l'autorisation de mettre à jour une définition de catalogue de signaux spécifique	Écrire	signalcatalog*		
UpdateStateTemplate	Accorde l'autorisation de mettre à jour le modèle d'état donné	Écrire	statetemplate*		
UpdateVehicle	Accorde l'autorisation de mettre à jour le véhicule	Écrire	vehicle*		
			decodermanifest		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			modelmanifest		
				iotfleetwise:UpdateToModelManifestArn iotfleetwise:UpdateToDecoderManifestArn	

Types de ressources définis par AWS l'IoT FleetWise

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
campaign	`arn:${Partition}:iotfleetwise:${Region}:${Account}:campaign/${CampaignName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
decodermanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:decoder-manifest/${Name}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:iotfleetwise:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}
modelmanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:model-manifest/${Name}	aws:ResourceTag/${TagKey}
signalcatalog	arn:${Partition}:iotfleetwise:${Region}:${Account}:signal-catalog/${Name}	aws:ResourceTag/${TagKey}
vehicle	arn:${Partition}:iotfleetwise:${Region}:${Account}:vehicle/${VehicleId}	aws:ResourceTag/${TagKey}
statetemplate	arn:${Partition}:iotfleetwise:${Region}:${Account}:state-template/${StateTemplateId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS l'IoT FleetWise

AWS L'IoT FleetWise définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
iotfleetwise:DestinationArn	Filtre l'accès par ARN de destination de campagne, par exemple, un ARN de compartiment S3 ou un ARN Timestream.	ARN
iotfleetwise:Signals	Filtre l'accès par des noms de signaux entièrement qualifiés	ArrayOfString
iotfleetwise:UpdateToDecoderManifestArn	Filtre l'accès par une liste de manifestes de FleetWise décodeurs IoT ARNs	ARN
iotfleetwise:UpdateToModelManifestArn	Filtre l'accès par une liste de manifestes de FleetWise modèles IoT ARNs	ARN

Actions, ressources et clés de condition pour AWS IoT Greengrass

AWS IoT Greengrass (préfixe de service :`greengrass`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Greengrass
- Types de ressources définis par AWS IoT Greengrass
- Clés de condition pour AWS IoT Greengrass

Actions définies par AWS IoT Greengrass

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateRoleToGroup	Accorde l'autorisation d'associer un rôle à un groupe. Les autorisations du rôle doivent permettre aux fonctions Lambda principales et aux connecteurs de Greengrass d'effectuer des actions dans d'autres services. AWS	Écrire	group*		
AssociateServiceRoleToAccount	Accorde l'autorisation d'associer un rôle à votre compte. AWS IoT Greengrass utilise ce rôle pour accéder à	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	vos fonctions Lambda et à vos ressources IoT AWS				
CreateConnectorDefinition	Accorde l'autorisation de créer une définition de connecteur	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorDefinitionVersion	Accorde l'autorisation de créer une version d'une définition de connecteur existante	Écriture	connectorDefinition*		
CreateCoreDefinition	Accorde l'autorisation de créer une définition de noyau	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreDefinitionVersion	Accorde l'autorisation de créer une version d'une définition de noyau existante. Les groupes Greengrass doivent contenir chacun exactement un noyau Greengrass	Écriture	coreDefinition*		
CreateDeployment	Accorde l'autorisation de créer un déploiement	Écriture	group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeviceDefinition	Accorde l'autorisation de créer une définition de périphérique	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceDefinitionVersion	Accorde l'autorisation de créer une version d'une définition de périphérique existante	Écriture	deviceDefinition*		
CreateFunctionDefinition	Accorde l'autorisation de créer une définition de fonction Lambda à utiliser dans un groupe qui contient la liste des fonctions Lambda et de leurs configurations	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionDefinitionVersion	Accorde l'autorisation de créer une version d'une définition de fonction Lambda existante	Écrire	functionDefinition*		
CreateGroup	Accorde l'autorisation de créer un groupe.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGroupCertificateAuthority	Accorde l'autorisation de créer une autorité de certification pour le groupe, ou de procéder à la rotation de l'autorité de certification existante	Écriture	group*		
CreateGroupVersion	Accorde l'autorisation de créer une version d'un groupe qui a déjà été défini	Écriture	group*		
CreateLoggerDefinition	Accorde l'autorisation de créer une définition d'enregistreur d'événements	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	Accorde l'autorisation de créer une version d'une définition d'enregistreur d'événements existante	Écriture	loggerDefinition*		
CreateResourceDefinition	Accorde l'autorisation de créer une définition de ressource qui contient la liste des ressources à utiliser dans un groupe	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateResourceDefinitionVersion	Accorde l'autorisation de créer une version d'une définition de ressource existante	Écrire	resourceDefinition*		
CreateSoftwareUpdateJob	Autorise la création d'une tâche AWS IoT qui incitera vos cœurs Greengrass à mettre à jour le logiciel qu'ils exécutent	Écrire			
CreateSubscriptionDefinition	Accorde l'autorisation de créer une définition d'abonnement	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionDefinitionVersion	Accorde l'autorisation de créer une version d'une définition d'abonnement existante	Écriture	subscriptionDefinition*		
DeleteConnectorDefinition	Accorde l'autorisation de supprimer une définition de connecteur	Écriture	connectorDefinition*		
DeleteCoreDefinition	Accorde l'autorisation de supprimer une définition de noyau. La suppression d'une définition en cours d'utilisation dans un déploiement affecte les déploiements à venir	Écriture	coreDefinition*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDeviceDefinition	Accorde l'autorisation de supprimer une définition de périphérique. La suppression d'une définition en cours d'utilisation dans un déploiement affecte les déploiements à venir	Écriture	deviceDefinition*		
DeleteFunctionDefinition	Accorde l'autorisation de supprimer une définition de fonction Lambda. La suppression d'une définition en cours d'utilisation dans un déploiement affecte les déploiements à venir	Écriture	functionDefinition*		
DeleteGroup	Accorde l'autorisation de supprimer un groupe qui n'est pas en cours d'utilisation dans un déploiement	Écriture	group*		
DeleteLoggerDefinition	Accorde l'autorisation de supprimer une définition d'enregistreur d'événements. La suppression d'une définition en cours d'utilisation dans un déploiement affecte les déploiements à venir	Écriture	loggerDefinition*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteResourceDefinition	Accorde l'autorisation de supprimer une définition de ressource	Écriture	resourceDefinition*		
DeleteSubscriptionDefinition	Accorde l'autorisation de supprimer une définition d'abonnement. La suppression d'une définition en cours d'utilisation dans un déploiement affecte les déploiements à venir	Écriture	subscriptionDefinition*		
DisassociateRoleFromGroup	Accorde l'autorisation de dissocier le rôle d'un groupe	Écriture	group*		
DisassociateServiceRoleFromAccount	Accorde l'autorisation de dissocier le rôle de service d'un compte. Sans rôle de service, les déploiements ne fonctionnent pas	Écriture			
Discover	Accorde l'autorisation de récupérer les informations requises pour se connecter à un noyau Greengrass	Lecture	thing*		
GetAssociatedRole	Accorde l'autorisation de récupérer le rôle associé à un groupe	Lecture	group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBulkDeploymentStatus	Accorde l'autorisation de renvoyer le statut d'un déploiement en bloc	Lecture	bulkDeployment*		
GetConnectivityInfo	Accorde l'autorisation de récupérer les informations de connectivité d'un noyau	Lecture	connectivityInfo*		
GetConnectorDefinition	Accorde l'autorisation de récupérer des informations sur une définition de connecteur	Lecture	connectorDefinition*		
GetConnectorDefinitionVersion	Accorde l'autorisation de récupérer des informations sur la version d'une définition de connecteur	Lecture	connectorDefinition*		
			connectorDefinitionVersion*		
GetCoreDefinition	Accorde l'autorisation de récupérer des informations sur une définition de noyau	Lecture	coreDefinition*		
GetCoreDefinitionVersion	Accorde l'autorisation de récupérer des informations sur la version d'une définition de noyau	Lecture	coreDefinition*		
			coreDefinitionVersion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDeploymentStatus	Accorde l'autorisation de renvoyer le statut d'un déploiement	Lecture	deployment*		
			group*		
GetDeviceDefinition	Accorde l'autorisation de récupérer des informations sur une définition de périphérique	Lecture	deviceDefinition*		
GetDeviceDefinitionVersion	Accorde l'autorisation de récupérer des informations sur la version d'une définition de périphérique	Lecture	deviceDefinition*		
			deviceDefinitionVersion*		
GetFunctionDefinition	Accorde l'autorisation de récupérer des informations sur une définition de fonction Lambda, telles que son heure de création et la version la plus récente	Lecture	functionDefinition*		
GetFunctionDefinitionVersion	Accorde l'autorisation de récupérer des informations sur la version d'une définition de fonction Lambda, telles que les fonctions Lambda incluses dans la version et leurs configurations	Lecture	functionDefinition*		
			functionDefinitionVersion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGroup	Accorde l'autorisation de récupérer des informations sur un groupe	Lecture	group*		
GetGroupCertificateAuthority	Accorde l'autorisation de renvoyer la clé publique de l'autorité de certification associée à un groupe	Lecture	certificateAuthority*		
			group*		
GetGroupCertificateConfiguration	Accorde l'autorisation de récupérer la configuration actuelle de l'autorité de certification utilisée par un groupe	Lecture	group*		
GetGroupVersion	Accorde l'autorisation de récupérer des informations sur la version d'un groupe	Lecture	group*		
			groupVersion*		
GetLoggerDefinition	Accorde l'autorisation de récupérer des informations sur une définition d'enregistreur d'événements	Lecture	loggerDefinition*		
GetLoggerDefinitionVersion	Accorde l'autorisation de récupérer des informations sur la version d'une définition d'enregistreur d'événements	Lecture	loggerDefinition*		
			loggerDefinitionVersion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourceDefinition	Accorde l'autorisation de récupérer des informations sur une définition de ressource, telles que son heure de création et la version la plus récente	Lecture	resourceDefinition*		
GetResourceDefinitionVersion	Accorde l'autorisation de récupérer des informations sur la version d'une définition de ressource, telles que les ressources incluses dans la version	Lecture	resourceDefinition*		
			resourceDefinitionVersion*		
GetServiceRoleForAccount	Accorde l'autorisation de récupérer le rôle de service attaché à un compte	Lecture			
GetSubscriptionDefinition	Accorde l'autorisation de récupérer des informations sur une définition d'abonnement	Lecture	subscriptionDefinition*		
GetSubscriptionDefinitionVersion	Accorde l'autorisation de récupérer des informations sur la version d'une définition d'abonnement	Lecture	subscriptionDefinition*		
			subscriptionDefinitionVersion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetThingRuntimeConfiguration	Accorde l'autorisation de récupérer la configuration d'exécution d'un objet	Lecture	thingRuntimeConfig*		
ListBulkDeploymentDetailedReports	Accorde l'autorisation de récupérer la liste paginée des déploiements qui ont été démarrés dans une opération de déploiement en bloc et leur statut de déploiement actuel	Lecture	bulkDeployment*		
ListBulkDeployments	Accorde l'autorisation de récupérer la liste des déploiements en bloc	Liste			
ListConnectorDefinitionVersions	Accorde l'autorisation de répertorier les versions d'une définition de connecteur	Liste	connectorDefinition*		
ListConnectorDefinitions	Accorde l'autorisation de récupérer une liste des définitions de connecteur	Liste			
ListCoreDefinitionVersions	Accorde l'autorisation de répertorier les versions d'une définition de noyau	Liste	coreDefinition*		
ListCoreDefinitions	Accorde l'autorisation de récupérer une liste des définitions de noyau	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDeployments	Accorde l'autorisation de récupérer une liste de tous les déploiements pour un groupe	Liste	group*		
ListDeviceDefinitionVersions	Accorde l'autorisation de répertorier les versions d'une définition de périphérique	Liste	deviceDefinition*		
ListDeviceDefinitions	Accorde l'autorisation de récupérer une liste des définitions de périphérique	Liste			
ListFunctionDefinitionVersions	Accorde l'autorisation de répertorier les versions d'une définition de fonction Lambda	Liste	functionDefinition*		
ListFunctionDefinitions	Accorde l'autorisation de récupérer une liste des définitions de fonction Lambda	List			
ListGroupCertificateAuthorities	Accorde l'autorisation de récupérer une liste des informations actuelles CAs pour un groupe	List	group*		
ListGroupVersions	Accorde l'autorisation de répertorier les versions d'un groupe	Liste	group*		
ListGroups	Accorde l'autorisation de récupérer une liste des groupes	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLoggerDefinitionVersions	Accorde l'autorisation de répertorier les versions d'une définition d'enregistreur d'événements	Liste	loggerDefinition*		
ListLoggerDefinitions	Accorde l'autorisation de récupérer une liste des définitions d'enregistreur d'événements	Liste			
ListResourceDefinitionVersions	Accorde l'autorisation de répertorier les versions d'une définition de ressource	Liste	resourceDefinition*		
ListResourceDefinitions	Accorde l'autorisation de récupérer une liste des définitions de ressource	Liste			
ListSubscriptionDefinitionVersions	Accorde l'autorisation de répertorier les versions d'une définition d'abonnement	Liste	subscriptionDefinition*		
ListSubscriptionDefinitions	Accorde l'autorisation de récupérer une liste des définitions d'abonnement	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	bulkDeployment		
			connectorDefinition		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetDeployments	Accorde l'autorisation de réinitialiser les déploiements d'un groupe	Écriture	group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartBulkDeployment	Accorde l'autorisation de déployer plusieurs groupes dans une opération	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
StopBulkDeployment	Accorde l'autorisation d'arrêter l'exécution d'un déploiement en bloc	Écriture	bulkDeployment*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Balisage	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			subscriptionDefinition		
				aws:TagKeys	
UpdateConnectivityInfo	Accorde l'autorisation de mettre à jour les informations de connectivité d'un noyau Greengrass. Tous les périphériques appartenant au groupe disposant de ce noyau reçoivent ces informations leur permettant de trouver l'emplacement du noyau et de s'y connecter	Écriture	connectivityInfo*		
UpdateConnectorDefinition	Accorde l'autorisation de mettre à jour une définition de connecteur	Écriture	connectorDefinition*		
UpdateCoreDefinition	Accorde l'autorisation de mettre à jour une définition de noyau	Écriture	coreDefinition*		
UpdateDeviceDefinition	Accorde l'autorisation de mettre à jour une définition de périphérique	Écriture	deviceDefinition*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFunctionDefinition	Accorde l'autorisation de mettre à jour une définition de fonction Lambda	Écriture	functionDefinition*		
UpdateGroup	Accorde l'autorisation de mettre à jour un groupe	Écriture	group*		
UpdateGroupCertificateConfiguration	Accorde l'autorisation de mettre à jour le délai d'expiration du certificat pour un groupe	Écriture	group*		
UpdateLoggerDefinition	Accorde l'autorisation de mettre à jour une définition d'enregistreur d'événements	Écriture	loggerDefinition*		
UpdateResourceDefinition	Accorde l'autorisation de mettre à jour une définition de ressource	Écriture	resourceDefinition*		
UpdateSubscriptionDefinition	Accorde l'autorisation de mettre à jour une définition d'abonnement	Écriture	subscriptionDefinition*		
UpdateThingRuntimeConfiguration	Accorde l'autorisation de mettre à jour la configuration d'exécution d'un objet	Écrire	thingRuntimeConfig*		

Types de ressources définis par AWS IoT Greengrass

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
certificateAuthority	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/certificateauthorities/${CertificateAuthorityId}`	
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}`	
bulkDeployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/bulk/deployments/${BulkDeploymentId}`	aws:ResourceTag/${TagKey}
group	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}`	aws:ResourceTag/${TagKey}
groupVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/versions/${VersionId}`	
coreDefinition	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}`	aws:ResourceTag/${TagKey}
coreDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/`	

Types de ressources	ARN	Clés de condition
	cores/${CoreDefinitionId}/versions/${VersionId}	
deviceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}	aws:ResourceTag/${TagKey}
deviceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}/versions/${VersionId}	
functionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}	aws:ResourceTag/${TagKey}
functionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}/versions/${VersionId}	
subscriptionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}	aws:ResourceTag/${TagKey}
subscriptionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}/versions/${VersionId}	
loggerDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
loggerDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}/versions/${VersionId}	
resourceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}	aws:ResourceTag/${TagKey}
resourceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}/versions/${VersionId}	
connectorDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}	aws:ResourceTag/${TagKey}
connectorDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}/versions/${VersionId}	
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
thingRuntimeConfig	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/runtimeconfig	

Clés de condition pour AWS IoT Greengrass

AWS IoT Greengrass définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur de balise associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS IoT Greengrass V2

AWS IoT Greengrass V2 (préfixe de service :`greengrass`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Greengrass V2
- Types de ressources définis par AWS IoT Greengrass V2
- Clés de condition pour AWS IoT Greengrass V2

Actions définies par AWS IoT Greengrass V2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateServiceRoleToAccount	Accorde l'autorisation d'associer un rôle à votre compte. AWS IoT Greengrass utilise ce rôle pour accéder à vos fonctions Lambda et à vos ressources IoT AWS	Gestion des autorisations			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	Accorde l'autorisation d'associer une liste d'appareils de client à un appareil principal	Écrire	coreDevice*		
BatchDisassociateClientDeviceFromCoreDevice	Accorde l'autorisation de dissocier une liste d'appareils de client d'un appareil principal	Écrire	coreDevice*		
CancelDeployment	Accorde l'autorisation d'annuler un déploiement	Écriture	deployment*		iot:CancelJob iot:DeleteThingShadow

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	Accorde l'autorisation de créer un composant	Écriture	component * *		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeployment	Accorde l'autorisation de créer un déploiement	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	iot:CancelJob iot:CreateJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
DeleteComponent	Accorde l'autorisation de supprimer un composant	Écrire	componentVersion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCoreDevice	Accorde l'autorisation de supprimer un appareil principal AWS IoT Greengrass, qui est un objet AWS IoT. Cette opération supprime l'appareil Core de la liste des appareils Core. Cette opération ne supprime pas l' AWS IoT	Écrire	coreDevice*		iot:DescribeJobExecution
DeleteDeployment	Accorde l'autorisation de supprimer un déploiement. Pour supprimer un déploiement actif, il est nécessaire de commencer par l'annuler	Écrire	deployment*		iot:DeleteJob
DescribeComponent	Accorde l'autorisation de récupérer les métadonnées d'une version d'un composant	Lecture	componentVersion*		
DisassociateServiceRoleFromAccount	Accorde l'autorisation de dissocier le rôle de service d'un compte. Sans rôle de service, les déploiements ne fonctionnent pas	Écrire			
GetComponent	Accorde l'autorisation d'obtenir une recette d'une version d'un composant	Lecture	componentVersion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetComponentVersionArtifact	Accorde l'autorisation de récupérer l'URL pré-signée pour télécharger un artefact de composant public	Lecture	componentVersion*		
GetConnectivityInfo	Accorde l'autorisation de récupérer les informations de connectivité d'un appareil noyau Greengrass	Lecture	connectivityInfo*		iot:GetThingShadow
GetCoreDevice	Accorde l'autorisation de récupérer les métadonnées d'un appareil AWS IoT Greengrass central	Lecture	coreDevice*		
GetDeployment	Accorde l'autorisation d'obtenir un déploiement	Lecture	deployment*		iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
GetServiceRoleForAccount	Accorde l'autorisation de récupérer le rôle de service attaché à un compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListClientDevicesAssociatedWithCoreDevice	Accorde l'autorisation de récupérer une liste paginée d'appareils clients associés à un appareil principal AWS IoT Greengrass	List	coreDevice*		
ListComponentVersions	Accorde l'autorisation de récupérer la liste paginée de toutes les versions d'un composant	Liste	component*		
ListComponents	Accorde l'autorisation de récupérer la liste paginée des résumés de composants	List			
ListCoreDevices	Autorise la récupération d'une liste paginée des principaux AWS appareils IoT Greengrass	List			
ListDeployments	Accorde l'autorisation de récupérer la liste paginée des déploiements	List			iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEffectiveDeployments	Autorise l'extraction d'une liste paginée des tâches de déploiement envoyées par IoT AWS Greengrass aux principaux appareils IoT AWS Greengrass	List	coreDevice*		iot:DescribeJob iot:DescribeJobExecution iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListInstalledComponents	Accorde l'autorisation de récupérer une liste paginée des composants exécutés par un appareil AWS IoT Greengrass principal	List	coreDevice*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	component		
			componentVersion		
			coreDevice		
			deployment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
ResolveComponentCandidates	Accorde l'autorisation de répertorier les composants qui répondent aux exigences d'un déploiement en matière de composants, de version et de plateforme	Liste	componentVersion*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource.	Balisage	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Balisage	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateConnectivityInfo	Accorde l'autorisation de mettre à jour les informations de connectivité d'un noyau Greengrass. Tous les périphériques appartenant au groupe disposant de ce noyau reçoivent ces informations leur permettant de trouver l'emplacement du noyau et de s'y connecter	Écrire	connectivityInfo*		iot:GetThingShadow iot:UpdateThingShadow

Types de ressources définis par AWS IoT Greengrass V2

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
component	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}`	aws:ResourceTag/${TagKey}
componentVersion	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}:versions:${ComponentVersion}`	aws:ResourceTag/${TagKey}
coreDevice	`arn:${Partition}:greengrass:${Region}:${Account}:coreDevices:${CoreDeviceThingName}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:deployments:${DeploymentId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS IoT Greengrass V2

AWS IoT Greengrass V2 définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en vérifiant les key/value paires de balises incluses dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en vérifiant les key/value paires de balises associées à une ressource spécifique	String
aws:TagKeys	Filtre l'accès en vérifiant les clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les emplois liés à AWS l'IoT DataPlane

AWS IoT Jobs DataPlane (préfixe de service :`iotjobsdata`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Jobs DataPlane
- Types de ressources définis par AWS IoT Jobs DataPlane
- Clés de condition pour les emplois AWS liés à l'IoT DataPlane

Actions définies par AWS IoT Jobs DataPlane

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeJobExecution	Accorde l'autorisation de décrire une exécution de tâche	Lecture	thing*		
				iot:JobId	
GetPendingJobExecutions	Accorde l'autorisation d'obtenir la liste de toutes les tâches d'un objet qui ne se trouvent pas dans un état terminal	Lecture	thing*		
StartNextPendingJobExecution	Accorde l'autorisation d'obtenir et de démarrer l'exécution de tâche en attente suivante pour un objet	Écrire	thing*		
UpdateJobExecution	Accorde l'autorisation de mettre à jour l'exécution d'une tâche	Écrire	thing*		
				iot:JobId	

Types de ressources définis par AWS IoT Jobs DataPlane

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	

Clés de condition pour les emplois AWS liés à l'IoT DataPlane

AWS IoT Jobs DataPlane définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
iot:JobId	Filtre l'accès par JoBid pour iotjobsdata : et iotjobsdata : DescribeJobExecution UpdateJobExecution APIs	String

Actions, ressources et clés de condition pour les intégrations gérées par AWS l'IoT

AWS IoT Managed Integrations (préfixe de service :`iotmanagedintegrations`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les intégrations gérées par AWS l'IoT
- Types de ressources définis par les intégrations gérées par AWS l'IoT
- Clés de condition pour les intégrations gérées par AWS l'IoT

Actions définies par les intégrations gérées par AWS l'IoT

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAccountAssociation	Accorde l'autorisation de créer une nouvelle association de comptes	Écrire		aws:RequestTag/${TagKey} aws:TagKeys iotmanagedintegrations:connectorDestinationId	
CreateCloudConnector	Accorde l'autorisation de créer un nouveau connecteur cloud	Écrire			
CreateConnectorDestination	Accorde l'autorisation de créer une nouvelle destination de connecteur	Écrire		iotmanagedintegrations:clou	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				dConnectorId	
CreateCredentialLocker	Accorde l'autorisation de créer un casier d'informations d'identification du produit	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDestination	Accorde l'autorisation de créer une nouvelle destination	Écrire			
CreateEventLogConfiguration	Accorde l'autorisation de créer une nouvelle configuration d'événement	Écrire			
CreateManagedThing	Accorde l'autorisation de créer un nouvel objet géré	Écrire	credential-locker		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationConfiguration	Accorde l'autorisation de créer une nouvelle configuration de notification	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOtaTask	Accorde l'autorisation de créer une nouvelle tâche ota	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOtaTaskConfiguration	Accorde l'autorisation de créer une nouvelle configuration de tâche ota	Écrire			
CreateProvisioningProfile	Accorde l'autorisation de créer un nouveau profil d'approvisionnement	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssociation	Accorde l'autorisation de supprimer une association de comptes	Écrire	account-association*		
DeleteCloudConnector	Autorise la suppression d'un connecteur cloud	Écrire		iotmanagedintegrations:cloudConnectorId	
DeleteConnectorDestination	Accorde l'autorisation de supprimer une destination de connecteur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCredentialLocker	Accorde l'autorisation de supprimer un casier d'informations d'identification	Écrire	credential-locker*		
DeleteDestination	Accorde l'autorisation de supprimer la destination	Écrire			
DeleteEventLogConfiguration	Accorde l'autorisation de supprimer la configuration du journal des événements	Écrire			
DeleteManagedThing	Accorde l'autorisation de supprimer un objet géré	Écrire	managed-thing*		
DeleteNotification Configuration	Accorde l'autorisation de supprimer la configuration des notifications	Écrire			
DeleteOtaTask	Accorde l'autorisation de supprimer une tâche ota	Écrire	ota-task*		
DeleteOtaTaskConfiguration	Autorise la suppression de la configuration des tâches ota	Écrire			
DeleteProvisioningProfile	Accorde l'autorisation de supprimer le profil d'approvisionnement	Écrire	provisioning-profile*		
DeregisterAccountAssociation	Accorde l'autorisation de désenregistrer une association de comptes	Écrire	account-association*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			managed-thing*		
GetAccountAssociation	Accorde l'autorisation d'obtenir des informations sur une association de comptes	Lecture	account-association*		
GetCloudConnector	Accorde l'autorisation d'obtenir des informations sur un connecteur cloud	Lecture			
GetConnectorDestination	Accorde l'autorisation d'obtenir des informations sur une destination cloud	Lecture			
GetCredentialLocker	Accorde l'autorisation d'obtenir des informations sur un casier d'identifiants	Lecture	credential-locker*		
GetCustomEndpoint	Accorde l'autorisation d'obtenir des informations sur un point de terminaison personnalisé	Lecture			
GetDefaultEncryptionConfiguration	Accorde l'autorisation d'obtenir des informations sur une configuration de chiffrement par défaut	Lecture			
GetDestination	Accorde l'autorisation d'obtenir des informations sur une destination	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDeviceDiscovery	Accorde l'autorisation d'obtenir des informations sur la découverte d'un appareil	Lecture			
GetEventLogConfiguration	Accorde l'autorisation d'obtenir des informations sur la configuration d'un journal d'événements	Lecture			
GetHubConfiguration	Accorde l'autorisation d'obtenir des informations sur la configuration d'un hub	Lecture			
GetManagedThing	Accorde l'autorisation d'obtenir des informations sur un objet géré	Lecture	managed-thing*		
GetManagedThingCapabilities	Accorde l'autorisation d'obtenir le rapport de capacité pour un objet géré	Lecture	managed-thing*		
GetManagedThingCertificate	Accorde l'autorisation d'obtenir le certificat pem pour un objet géré	Lecture	managed-thing*		
GetManagedThingConnectivityData	Accorde l'autorisation d'obtenir les données de connectivité d'un objet géré	Lecture	managed-thing*		
GetManagedThingMetaData	Accorde l'autorisation d'obtenir les informations de métadonnées pour un objet géré	Lecture	managed-thing*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetManagedThingState	Accorde l'autorisation d'obtenir les informations sur l'état de l'appareil pour un objet géré	Lecture	managed-thing*		
GetNotificationConfiguration	Accorde l'autorisation d'obtenir des informations pour une configuration de notification	Lecture			
GetOtaTask	Accorde l'autorisation d'obtenir des informations pour une tâche ota	Lecture	ota-task*		
GetOtaTaskConfiguration	Accorde l'autorisation d'obtenir des informations pour la configuration d'une tâche ota	Lecture			
GetProvisioningProfile	Accorde l'autorisation d'obtenir des informations pour un profil d'approvisionnement	Lecture	provisioning-profile*		
GetRuntimeLogConfiguration	Accorde l'autorisation d'obtenir des informations pour la configuration d'un journal d'exécution	Lecture			
GetSchemaVersion	Accorde l'autorisation d'obtenir des informations pour une version d'un schéma	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAccountAssociations	Accorde l'autorisation de répertorier des informations pour les associations de comptes	List			
ListCloudConnectors	Accorde l'autorisation de répertorier les informations pour les connecteurs cloud	List			
ListConnectorDestinations	Accorde l'autorisation de répertorier les informations relatives aux destinations des connecteurs	List			
ListCredentialLockers	Accorde l'autorisation de répertorier des informations pour les casiers d'identifiants	List			
ListDestinations	Accorde l'autorisation de répertorier les informations relatives aux destinations	List			
ListDeviceDiscoveries	Accorde l'autorisation de répertorier les informations relatives à la découverte d'appareils	List			
ListDiscoveredDevices	Accorde l'autorisation de répertorier les informations relatives à l'appareil découvert lors de la découverte d'un appareil	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEventLogConfigurations	Accorde l'autorisation de répertorier les informations pour les configurations du journal des événements	Lecture			
ListManagedThingAccountAssociations	Accorde l'autorisation de répertorier les informations relatives aux associations entre les objets gérés et les associations de comptes	List			
ListManagedThingSchemas	Accorde l'autorisation de répertorier les schémas associés à un objet géré	Lecture	managed-thing*		
ListManagedThings	Accorde l'autorisation de répertorier les informations relatives aux objets gérés	List			
ListNotificationConfigurations	Accorde l'autorisation de répertorier les informations pour les configurations de notification	Lecture			
ListOtaTaskConfigurations	Accorde l'autorisation de répertorier les informations pour les configurations de tâches ota	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOtaTaskExecutions	Accorde l'autorisation de répertorier les informations pour les exécutions de tâches ota	Lecture	ota-task*		
ListOtaTasks	Accorde l'autorisation de répertorier les informations pour les tâches OTA	List			
ListProvisioningProfiles	Accorde l'autorisation de répertorier les informations pour les profils d'approvisionnement	List			
ListSchemaVersions	Accorde l'autorisation de répertorier les informations relatives aux schémas	List			
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée.	Lecture	account-association		
			credential-locker		
			managed-thing		
			ota-task		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			provisioning-profile		
				aws:ResourceTag/${TagKey}	
PutDefaultEncryptionConfiguration	Accorde l'autorisation de mettre à jour les paramètres par défaut d'une configuration de chiffrement	Écrire			
PutHubConfiguration	Accorde l'autorisation de mettre à jour la configuration d'un hub	Écrire			
PutRuntimeLogConfiguration	Accorde l'autorisation de mettre à jour la configuration d'un journal d'exécution	Écrire			
RegisterAccountAssociation	Accorde l'autorisation d'enregistrer une association de compte à un objet géré	Écrire	account-association*		
			managed-thing*		
RegisterCustomEndpoint	Accorde l'autorisation d'enregistrer un point de terminaison personnalisé	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResetRuntimeLogConfiguration	Accorde l'autorisation de réinitialiser la configuration d'un journal d'exécution	Écrire			
SendConnectorEvent	Accorde l'autorisation d'envoyer un événement de connecteur	Écrire			
SendManagedThingCommand	Accorde l'autorisation d'envoyer une commande à un objet géré	Écrire	managed-thing*		
			account-association		
StartAccountAssociationRefresh	Accorde l'autorisation de démarrer une actualisation des jetons d'accès associés à une association de comptes	Écrire	account-association*		
StartDeviceDiscovery	Accorde l'autorisation de démarrer la découverte d'un appareil	Écrire	account-association		
			managed-thing		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter des balises pour la ressource spécifiée	Identification	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises pour la ressource spécifiée	Identification	account-association		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAccountAssociation	Autorise la mise à jour d'une association de comptes	Écrire	account-association*		
UpdateCloudConnector	Autorise la mise à jour d'un connecteur cloud	Écrire		iotmanagedintegrations:cloudConnectorId	
UpdateConnectorDestination	Accorde l'autorisation de mettre à jour la destination d'un connecteur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDestination	Accorde l'autorisation de mettre à jour une destination	Écrire			
UpdateEventLogConfiguration	Accorde l'autorisation de mettre à jour la configuration d'un journal d'événements	Écrire			
UpdateManagedThing	Accorde l'autorisation de mettre à jour un objet géré	Écrire	managed-thing*		
			credential-locker		
UpdateNotificationConfiguration	Accorde l'autorisation de mettre à jour une configuration de notification	Écrire			
UpdateOtaTask	Autorise la mise à jour d'une tâche ota	Écrire	ota-task*		

Types de ressources définis par les intégrations gérées par AWS l'IoT

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
account-association	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:account-association/${AccountAssociationId}	aws:ResourceTag/${TagKey}
credential-locker	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:credential-locker/${Identifier}	aws:ResourceTag/${TagKey}
managed-thing	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:managed-thing/${Identifier}	aws:ResourceTag/${TagKey}
ota-task	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:ota-task/${Identifier}	aws:ResourceTag/${TagKey}
provisioning-profile	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:provisioning-profile/${Identifier}	aws:ResourceTag/${TagKey}

Clés de condition pour les intégrations gérées par AWS l'IoT

AWS IoT Managed Integrations définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString
iotmanagedintegrations:cloudConnectorId	Filtre l'accès par CloudConnectorId	String
iotmanagedintegrations:connectorDestinationId	Filtre l'accès par ConnectorDestinationId	String

Actions, ressources et clés de condition pour AWS l'IoT SiteWise

AWS L'IoT SiteWise (préfixe de service :`iotsitewise`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l' AWS IoT SiteWise
- Types de ressources définis par AWS l'IoT SiteWise
- Clés de condition pour AWS l'IoT SiteWise

Actions définies par l' AWS IoT SiteWise

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAssets	Accorde l'autorisation d'associer une ressource enfant à une ressource parent par une hiérarchie	Écrire	asset*		
AssociateTimeSeriesToAssetProperty	Accorde l'autorisation d'associer une série temporelle à la propriété d'une ressource	Écrire	asset*		
			time-series*		
BatchAssociateProjectAssets	Accorde l'autorisation d'associer des ressources à un projet	Écriture	project*		
BatchDisassociateProjectAssets	Accorde l'autorisation de dissocier des ressources d'un projet	Écrire	project*		
BatchGetAssetPropertyAggregates	Accorde l'autorisation de récupérer des agrégats calculés pour plusieurs propriétés de ressources	Lecture	asset		
			time-series		
	Accorde l'autorisation de récupérer la dernière valeur	Lecture	asset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetAssetPropertyValue	pour plusieurs propriétés de ressources		time-series		
BatchGetAssetPropertyValueHistory	Accorde l'autorisation de récupérer l'historique des valeurs pour plusieurs propriétés de ressources	Lecture	asset		
			time-series		
BatchPutAssetPropertyValue	Accorde l'autorisation de mettre des valeurs de propriété pour les propriétés de ressource	Écriture	asset		
			time-series		
CreateAccessPolicy	Accorde l'autorisation de créer une politique d'accès pour un portail ou un projet	Écriture	portal		
			project		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAsset	Accorde l'autorisation de créer une ressource à partir d'un modèle de ressource	Écriture	asset-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModel	Accorde l'autorisation de créer un modèle de ressource	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModelCompositeModel	Octroie l'autorisation de créer un modèle composite de ressource à l'intérieur d'un modèle de ressource.	Écrire	asset-model*		
CreateBulkImportJob	Accorde l'autorisation de créer une tâche d'importation en masse	Écrire			
CreateComputationModel	Autorise la création d'un modèle de calcul	Écrire	asset asset-model		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Accorde l'autorisation de créer un tableau de bord dans un projet	Écrire	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Accorde l'autorisation de créer un jeu de données.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	Accorde l'autorisation de créer une passerelle	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePortal	Accorde l'autorisation de créer un portail	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
CreateProject	Accorde l'autorisation de créer un projet dans un portail	Écriture	portal*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPolicy	Accorde l'autorisation de supprimer une politique d'accès	Écriture	access-policy*		
DeleteAsset	Accorde l'autorisation de supprimer une ressource	Écriture	asset*		
DeleteAssetModel	Accorde l'autorisation de supprimer un modèle de ressource	Écrire	asset-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAssetModelCompositeModel	Octroie l'autorisation de supprimer un modèle composite de ressource.	Écrire	asset-model*		
DeleteAssetModelInterfaceRelationship	Accorde l'autorisation de supprimer une relation entre le modèle d'actif et l'interface	Écrire	asset-model*		
DeleteComputationModel	Autorise la suppression d'un modèle de calcul	Écrire	computation-model*		
DeleteDashboard	Accorde l'autorisation de supprimer un tableau de bord	Écrire	dashboard*		
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données.	Écrire	dataset*		
DeleteGateway	Accorde l'autorisation de supprimer une passerelle	Écriture	gateway*		
DeletePortal	Accorde l'autorisation de supprimer un portail	Écriture	portal*		sso:DeleteManagedApplicationInstance
DeleteProject	Accorde l'autorisation de supprimer un projet	Écrire	project*		
DeleteTimeSeries		Écrire	asset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de supprimer une série temporelle		time-series		
DescribeAccessPolicy	Accorde l'autorisation de décrire une politique d'accès	Lecture	access-policy*		
DescribeAction	Octroie l'autorisation de décrire des actions.	Lecture	asset		
			computation-model		
DescribeAsset	Accorde l'autorisation de décrire une ressource	Lecture	asset*		
DescribeAssetCompositeModel	Octroie l'autorisation de décrire un modèle composite de ressource.	Lecture	asset*		
DescribeAssetModel	Accorde l'autorisation de décrire un modèle de ressource	Lecture	asset-model*		
DescribeAssetModelCompositeModel	Octroie l'autorisation de décrire un modèle composite de ressource.	Lecture	asset-model*		
DescribeAssetModelInterfaceRelationship	Accorde l'autorisation de décrire une relation entre le modèle d'actif et l'interface	Lecture	asset-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAssetProperty	Accorde l'autorisation de décrire une propriété de ressource	Lecture	asset*		
DescribeBulkImportJob	Accorde l'autorisation de décrire une tâche d'importation en masse	Lecture			
DescribeComputationModel	Autorise la description d'un modèle de calcul	Lecture	computation-model*		
DescribeComputationModelExecutionSummary	Autorise à décrire le résumé de l'exécution du modèle de calcul	Lecture	computation-model*		
			asset		
DescribeDashboard	Accorde l'autorisation de décrire un tableau de bord	Lecture	dashboard*		
DescribeDataset	Accorde l'autorisation de décrire l'ensemble de données	Lecture	dataset*		
DescribeDefaultEncryptionConfiguration	Accorde l'autorisation de décrire la configuration de chiffrement par défaut pour Compte AWS	Lecture			
DescribeExecution	Accorde l'autorisation de décrire une exécution	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeGateway	Accorde l'autorisation de décrire une passerelle	Lecture	gateway*		
DescribeGatewayCapabilityConfiguration	Accorde l'autorisation de décrire une configuration de capacité pour une passerelle	Lecture	gateway*		
DescribeLoggingOptions	Accorde l'autorisation de décrire les options de journalisation pour Compte AWS	Lecture			
DescribePortal	Accorde l'autorisation de décrire un portail	Lecture	portal*		
DescribeProject	Accorde l'autorisation de décrire un projet	Lecture	project*		
DescribeStorageConfiguration	Accorde l'autorisation de décrire la configuration de stockage pour le Compte AWS	Lecture			
DescribeTimeSeries	Accorde l'autorisation de décrire une série temporelle	Lecture	asset		
			time-series		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateAssets	Accorde l'autorisation de dissocier une ressource enfant d'une ressource parent par une hiérarchie	Écrire	asset*		
DisassociateTimeSeriesFromAssetProperty	Accorde l'autorisation de dissocier une série temporelle de la propriété d'une ressource	Écrire	asset*		
			time-series*		
EnableSiteWiseIntegration [autorisation uniquement]	Autorise l' SiteWise intégration de l'IoT à d'autres services	Écrire			
ExecuteAction	Octroie l'autorisation d'exécuter des actions.	Écrire	asset		
			computation-model		
ExecuteQuery	Accorde l'autorisation d'exécuter une requête	Lecture			
GetAssetPropertyAggregates	Accorde l'autorisation de récupérer des agrégats calculés pour une propriété de ressource	Lecture	asset		
			time-series		
GetAssetPropertyValue	Accorde l'autorisation de récupérer la dernière valeur d'une propriété de ressource	Lecture	asset		
			time-series		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAssetPropertyValueHistory	Accorde l'autorisation de récupérer l'historique des valeurs d'une propriété de ressource	Lecture	asset		
			time-series		
GetInterpolatedAssetPropertyValues	Accorde l'autorisation de récupérer les valeurs interpolées de la propriété d'une ressource	Lecture	asset		
			time-series		
InvokeAssistant	Accorde l'autorisation d'invoquer un assistant	Lecture			
ListAccessPolicies	Accorde l'autorisation de répertorier toutes les stratégies d'accès pour une identité ou une ressource	List	portal		
			project		
ListActions	Octroie l'autorisation de répertorier toutes les actions.	List	asset		
			computation-model		
ListAssetModelCompositeModels	Octroie l'autorisation de répertorier tous les modèles composites de ressource.	List	asset-model*		
ListAssetModelProperties	Accorde l'autorisation de répertorier tous les modèles de ressource	List	asset-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAssetModels	Accorde l'autorisation de répertorier tous les modèles de ressource	List			
ListAssetProperties	Octroie l'autorisation de répertorier les propriétés des actifs	List	asset*		
ListAssetRelationships	Accorde l'autorisation de répertorier le graphique des relations d'une ressource	Liste	asset*		
ListAssets	Accorde l'autorisation de répertorier toutes les ressources	List	asset-model		
ListAssociatedAssets	Accorde l'autorisation de répertorier toutes les ressources associées à une ressource par une hiérarchie	List	asset*		
ListBulkImportJobs	Accorde l'autorisation de répertorier les tâches d'importation en masse	List			
ListCompositionRelationships	Octroie l'autorisation de répertorier toutes les relations de modèles composites de ressource.	List	asset-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListComputationModelDataBindingUsages	Autorise à répertorier les utilisations de liaison de données des modèles de calcul	List	asset asset-model		
ListComputationModelResolveToResources	Autorise les ressources à répertorier la résolution du modèle de calcul	List	computation-model*		
ListComputationModels	Permet de répertorier tous les modèles de calcul	List			
ListDashboards	Accorde l'autorisation de répertorier tous les tableaux de bord d'un projet	List	project*		
ListDatasets	Accorde l'autorisation de répertorier tous les jeux de données.	List			
ListExecutions	Permet de répertorier les exécutions	List	asset computation-model		
ListGateways	Accorde l'autorisation de répertorier toutes les passerelles	List			
ListInterfaceRelationships	Permet de répertorier tous les modèles d'actifs appliqués par une interface	List	asset-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPortals	Accorde l'autorisation de répertorier tous les portails	Liste			
ListProjectAssets	Accorde l'autorisation de répertorier toutes les ressources associées à un projet	Liste	project*		
ListProjects	Accorde l'autorisation de répertorier tous les projets d'un portail	Liste	portal*		
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises pour une ressource	Lecture	access-policy		
			asset		
			asset-model		
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			time-series		
				aws:ResourceTag/${TagKey}	
ListTimeSeries	Accorde l'autorisation de répertorier les séries temporelles	List	asset		
PutAssetModelInterfaceRelationship	Accorde l'autorisation de créer une relation entre le modèle d'actif et l'interface	Écrire	asset-model*		
PutDefaultEncryptionConfiguration	Accorde l'autorisation de définir la configuration de chiffrement par défaut pour Compte AWS	Écrire			
PutLoggingOptions	Accorde l'autorisation de définir les options de journalisation pour Compte AWS	Écrire			
PutStorageConfiguration	Accorde l'autorisation de configurer les paramètres de stockage pour Compte AWS	Écrire			
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	access-policy		
			asset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			asset-model		
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	access-policy		
			asset		
			asset-model		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	Accorde l'autorisation de mettre à jour une politique d'accès	Écriture	access-policy*		
UpdateAsset	Accorde l'autorisation de mettre à jour une ressource	Écriture	asset*		
UpdateAssetModel	Accorde l'autorisation de mettre à jour un modèle de ressource	Écrire	asset-model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAssetModelCompositeModel	Octroie l'autorisation de mettre à jour un modèle composite de ressource.	Écrire	asset-model*		
UpdateAssetModelPropertyRouting [autorisation uniquement]	Accorde l'autorisation de mettre à jour le routage d'une AssetModel propriété	Écrire	asset-model*		
UpdateAssetProperty	Accorde l'autorisation de mettre à jour une propriété de ressource	Écrire	asset*		
UpdateComputationModel	Autorise la mise à jour d'un modèle de calcul	Écrire	computation-model*		
			asset		
			asset-model		
UpdateDashboard	Accorde l'autorisation de mettre à jour un tableau de bord	Écrire	dashboard*		
UpdateDataset	Accorde l'autorisation de mettre à jour un jeu de données.	Écrire	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGateway	Accorde l'autorisation de mettre à jour une passerelle	Écriture	gateway*		
UpdateGatewayCapabilityConfiguration	Accorde l'autorisation de mettre à jour une configuration de capacité pour une passerelle	Écriture	gateway*		
UpdatePortal	Accorde l'autorisation de mettre à jour un portail	Écriture	portal*		
UpdateProject	Accorde l'autorisation de mettre à jour un projet	Écrire	project*		

Types de ressources définis par AWS l'IoT SiteWise

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
asset	`arn:${Partition}:iotsitewise:${Region}:${Account}:asset/${AssetId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
asset-model	arn:${Partition}:iotsitewise:${Region}:${Account}:asset-model/${AssetModelId}	aws:ResourceTag/${TagKey}
time-series	arn:${Partition}:iotsitewise:${Region}:${Account}:time-series/${TimeSeriesId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:iotsitewise:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
portal	arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:iotsitewise:${Region}:${Account}:project/${ProjectId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:iotsitewise:${Region}:${Account}:dashboard/${DashboardId}	aws:ResourceTag/${TagKey}
access-policy	arn:${Partition}:iotsitewise:${Region}:${Account}:access-policy/${AccessPolicyId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:iotsitewise:${Region}:${Account}:dataset/${DatasetId}	aws:ResourceTag/${TagKey}
computation-model	arn:${Partition}:iotsitewise:${Region}:${Account}:computation-model/${ComputationModelId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS l'IoT SiteWise

AWS L'IoT SiteWise définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource	String
aws:TagKeys	Filtrer l'accès en fonction des clés de balise dans la demande	ArrayOfString
iotsitewise:assetHierarchyPath	Filtre l'accès selon un chemin de hiérarchie des actifs, qui est la chaîne des actifs IDs dans la hiérarchie des actifs, chacun étant séparé par une barre oblique	String
iotsitewise:childAssetId	Filtre l'accès en fonction de l'ID d'une ressource enfant associé à une ressource parent	String
iotsitewise:group	Filtre l'accès en fonction de l'ID d'un AWS groupe d'authentification unique	String
iotsitewise:iam	Filtre l'accès en fonction de l'ID d'une identité AWS IAM	String
iotsitewise:isAssociatedWithAssetProperty	Filtre l'accès en fonction des flux de données associés ou non aux propriétés de la ressource	String

Clés de condition	Description	Type
iotsitewise:portal	Filtre l'accès en fonction de l'ID d'un portail	Chaîne
iotsitewise:project	Filtre l'accès en fonction de l'ID d'un projet	String
iotsitewise:propertyAlias	Filtre l'accès en fonction de l'alias de propriété	String
iotsitewise:propertyId	Filtre l'accès en fonction de l'ID d'une propriété de ressource	String
iotsitewise:user	Filtre l'accès en fonction de l'identifiant d'un utilisateur AWS Single Sign-On	String

Actions, ressources et clés de condition pour AWS l'IoT TwinMaker

AWS L'IoT TwinMaker (préfixe de service :`iottwinmaker`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l' AWS IoT TwinMaker
- Types de ressources définis par AWS l'IoT TwinMaker
- Clés de condition pour AWS l'IoT TwinMaker

Actions définies par l' AWS IoT TwinMaker

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchPutPropertyValues	Accorde l'autorisation de définir des valeurs pour plusieurs propriétés de séries temporelles	Écrire	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			entity		
CancelMetadataTransferJob	Octroie l'autorisation d'annuler une tâche de transfert de métadonnées.	Écrire	metadataTransferJob*		
CreateComponentType	Accorde l'autorisation de créer un type de composant	Écrire	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEntity	Accorde l'autorisation de créer une entité	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetadataTransferJob	Octroie l'autorisation de créer une tâche de transfert de métadonnées.	Écrire			
CreateScene	Accorde l'autorisation de créer une scène	Écrire	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncJob	Accorde l'autorisation de créer une tâche de synchronisation	Écrire	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkspace	Accorde l'autorisation de créer un espace de travail	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponentType	Accorde l'autorisation de supprimer un type de composant	Écrire	componentType*		
			workspace*		
DeleteEntity	Accorde l'autorisation de supprimer une entité	Écrire	entity*		
			workspace*		
DeleteScene	Accorde l'autorisation de supprimer une scène	Écrire	scene*		
			workspace*		
DeleteSyncJob	Accorde l'autorisation de supprimer une tâche de synchronisation	Écrire	syncJob*		
			workspace*		
DeleteWorkspace	Accorde l'autorisation de supprimer un espace de travail.	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExecuteQuery	Accorde l'autorisation d'exécuter une requête	Lecture	workspace*		
GetComponentType	Accorde l'autorisation d'obtenir un type de composant	Lecture	componentType*		
			workspace*		
GetEntity	Accorde l'autorisation d'obtenir une entité	Lecture	entity*		
			workspace*		
GetMetadataTransferJob	Octroie l'autorisation d'obtenir une tâche de transfert de métadonnées.	Lecture	metadataTransferJob*		
GetPricingPlan	Accorde l'autorisation d'obtenir un plan de tarification	Lecture			
GetPropertyValue	Accorde l'autorisation de récupérer les valeurs de propriété	Lecture	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			componentType		
			entity		
GetPropertyValueHistory	Accorde l'autorisation de récupérer l'historique des valeurs d'une série temporelle	Lecture	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		
GetScene	Accorde l'autorisation d'obtenir une scène	Lecture	scene*		
			workspace*		
GetSyncJob	Accorde l'autorisation d'obtenir une tâche de synchronisation	Lecture	syncJob*		
			workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkspace	Accorde l'autorisation d'obtenir un espace de travail	Lecture	workspace*		
ListComponentTypes	Accorde l'autorisation de répertorier tous les types de composants d'un espace de travail	List	workspace*		
ListComponents	Octroie l'autorisation de répertorier les composants attachés à une entité.	List	entity*		
			workspace*		
ListEntities	Accorde l'autorisation de répertorier toutes les entités d'un espace de travail	List	workspace*		
ListMetadataTransferJobs	Octroie l'autorisation de répertorier toutes les tâches de transfert de métadonnées.	List			
ListProperties	Octroie l'autorisation de répertorier les propriétés d'un composant d'identité.	List	entity*		
			workspace*		
ListScenes	Accorde l'autorisation de répertorier toutes les scènes d'un espace de travail	List	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSyncJobs	Accorde l'autorisation de répertorier toutes les tâches de synchronisation d'un espace de travail	List	workspace*		
ListSyncResources	Accorde l'autorisation de répertorier toutes les ressources de synchronisation d'une tâche de synchronisation	List	syncJob*		
			workspace*		
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises pour une ressource	List	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:ResourceTag/${TagKey}	
ListWorkspaces	Accorde l'autorisation de répertorier tous les espaces de travail	List			
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	componentType		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			entity		
			scene		
			syncJob		
			workspace		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:TagKeys	
UpdateComponentType	Accorde l'autorisation de mettre à jour un type de composant	Écrire	componentType*		
			workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEntity	Accorde l'autorisation de mettre à jour une entité	Écrire	entity*		
			workspace*		
UpdatePricingPlan	Accorde l'autorisation de mettre à jour le plan de tarification	Écrire			
UpdateScene	Accorde l'autorisation de mettre à jour une scène	Écrire	scene*		
			workspace*		
UpdateWorkspace	Accorde l'autorisation de mettre à jour un espace de travail	Écrire	workspace*		

Types de ressources définis par AWS l'IoT TwinMaker

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workspace	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
entity	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/entity/${EntityId}	aws:ResourceTag/${TagKey}
componentType	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/component-type/${ComponentTypeId}	aws:ResourceTag/${TagKey}
scene	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/scene/${SceneId}	aws:ResourceTag/${TagKey}
syncJob	arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/sync-job/${SyncJobId}	aws:ResourceTag/${TagKey}
metadataTransferJob	arn:${Partition}:iottwinmaker:${Region}:${Account}:metadata-transfer-job/${MetadataTransferJobId}	

Clés de condition pour AWS l'IoT TwinMaker

AWS L'IoT TwinMaker définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource	String
aws:TagKeys	Filtrer l'accès en fonction des clés de balise dans la demande	ArrayOfString
iottwinmaker:destinationType	Filtre l'accès par type de destination de la tâche de transfert de métadonnées.	ArrayOfString
iottwinmaker:linkedServices	Filtre l'accès par espace de travail lié aux services.	ArrayOfString
iottwinmaker:sourceType	Filtre l'accès par type source de la tâche de transfert de métadonnées.	ArrayOfString

Actions, ressources et clés de condition pour AWS IoT Wireless

AWS IoT Wireless (préfixe de service :`iotwireless`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IoT Wireless

- Types de ressources définis par AWS IoT Wireless
- Clés de condition pour AWS IoT Wireless

Actions définies par AWS IoT Wireless

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateAwsAccountWithPartnerAccount	Accorde l'autorisation de lier les comptes partenaires à Compte AWS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateMulticastGroupWithFuotaTask	Accorde l'autorisation de les MulticastGroup associer à FuotaTask	Écrire	FuotaTask* MulticastGroup*		
AssociateWirelessDeviceWithFuotaTask	Accorde l'autorisation d'associer le périphérique sans fil à FuotaTask	Écrire	FuotaTask* WirelessDevice*		
AssociateWirelessDeviceWith	Accorde l'autorisation de les WirelessDevice associer à MulticastGroup	Écrire	MulticastGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
MulticastGroup			WirelessDevice*		
AssociateWirelessDeviceWithThing	Accorde l'autorisation d'associer l'appareil sans fil à un objet AWS IoT pour une période donnée wirelessDeviceId	Écrire	WirelessDevice* thing*		iot:DescribeThing
AssociateWirelessGatewayWithCertificate	Accorde l'autorisation d' WirelessGateway associer un certificat à l'IoT Core Identity	Écrire	WirelessGateway* cert*		
AssociateWirelessGatewayWithThing	Accorde l'autorisation d'associer la passerelle sans fil à un objet AWS IoT pour un objet donné wirelessGatewayId	Écrire	WirelessGateway* thing*		iot:DescribeThing
CancelMulticastGroupSession	Autorise l'annulation de la MulticastGroup session	Écrire	MulticastGroup*		
CreateDestination	Accorde l'autorisation de créer une ressource Destination.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeviceProfile	Accorde l'autorisation de créer une DeviceProfile ressource	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFuotaTask	Accorde l'autorisation de créer une FuotaTask ressource	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMulticastGroup	Accorde l'autorisation de créer une MulticastGroup ressource	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkAnalyzerConfiguration	Accorde l'autorisation de créer une NetworkAnalyzerConfiguration ressource	Écrire	MulticastGroup*		
			WirelessDevice*		
			WirelessGateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceProfile	Accorde l'autorisation de créer une ServiceProfile ressource	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessDevice	Accorde l'autorisation de créer une WirelessDevice ressource avec une destination donnée	Écrire	Destination		
			DeviceProfile		
			ServiceProfile		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWirelessGateway	Accorde l'autorisation de créer une WirelessGateway ressource	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGatewayTask	Accorde l'autorisation de créer une tâche pour une tâche donnée WirelessGateway	Écrire	WirelessGateway*		
CreateWirelessGatewayTaskDefinition	Accorde l'autorisation de créer une définition de WirelessGateway tâche	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDestination	Accorde l'autorisation de supprimer une destination.	Écrire	Destination*		
DeleteDeviceProfile	Accorde l'autorisation de supprimer un DeviceProfile	Écrire	DeviceProfile*		
DeleteFuotaTask	Accorde l'autorisation de supprimer le FuotaTask	Écrire	FuotaTask*		
DeleteMulticastGroup	Accorde l'autorisation de supprimer le MulticastGroup	Écrire	MulticastGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteNetworkAnalyzerConfiguration	Accorde l'autorisation de supprimer le NetworkAnalyzerConfiguration	Écrire	NetworkAnalyzerConfiguration*		
DeleteQueuedMessages	Accorde l'autorisation de suppression QueuedMessages	Écrire			
DeleteServiceProfile	Accorde l'autorisation de supprimer un ServiceProfile	Écrire	ServiceProfile*		
DeleteWirelessDevice	Accorde l'autorisation de supprimer un WirelessDevice	Écrire	WirelessDevice*		
DeleteWirelessDeviceImportTask	Octroie l'autorisation de supprimer la tâche d'importation de périphériques sans fil	Écrire	ImportTask*		
DeleteWirelessGateway	Accorde l'autorisation de supprimer un WirelessGateway	Écrire	WirelessGateway*		
DeleteWirelessGatewayTask	Accorde l'autorisation de supprimer une tâche pour une tâche donnée WirelessGateway	Écrire	WirelessGateway*		
DeleteWirelessGatewayTaskDefinition	Accorde l'autorisation de supprimer une définition de WirelessGateway tâche	Écrire	WirelessGatewayTaskDefinition*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterWirelessDevice	Accorde l'autorisation d'annuler l'enregistrement d'un périphérique sans fil	Écrire	WirelessDevice*		
DisassociateAwsAccountFromPartnerAccount	Permet de dissocier un compte Compte AWS d'un partenaire	Écrire	SidewalkAccount*		
DisassociateMulticastGroupFromFuotaTask	Accorde l'autorisation de dissocier le MulticastGroup FuotaTask	Écrire	FuotaTask*		
			MulticastGroup*		
DisassociateWirelessDeviceFromFuotaTask	Accorde l'autorisation de dissocier le périphérique sans fil de FuotaTask	Écrire	FuotaTask*		
			WirelessDevice*		
DisassociateWirelessDeviceFromMulticastGroup	Accorde l'autorisation de dissocier le périphérique sans fil de MulticastGroup	Écrire	MulticastGroup*		
			WirelessDevice*		
DisassociateWirelessDeviceFromThing	Permet de dissocier un appareil sans fil d'un objet AWS IoT	Écrire	WirelessDevice*		iot:DescribeThing
			thing*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateWirelessGatewayFromCertificate	Accorde l'autorisation de dissocier un certificat WirelessGateway IoT Core Identity d'un certificat	Écrire	WirelessGateway*		
			cert*		
DisassociateWirelessGatewayFromThing	Accorde l'autorisation WirelessGateway de dissocier un objet IoT Core	Écrire	WirelessGateway*		iot:DescribeThing
			thing*		
GetDestination	Accorde l'autorisation d'obtenir la destination.	Lecture	Destination*		
GetDeviceProfile	Accorde l'autorisation d'obtenir le DeviceProfile	Lire	DeviceProfile*		
GetEventConfigurationByResourceTypes	Accorde l'autorisation d'obtenir la configuration d'événements par types de ressources	Lecture			
GetFuotaTask	Accorde l'autorisation d'obtenir le FuotaTask	Lecture	FuotaTask*		
GetLogLevelsByResourceTypes	Accorde l'autorisation d'obtenir des niveaux de journal par type de ressource	Lecture			
GetMetricConfiguration	Accorde l'autorisation d'obtenir la configuration des métriques	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMetrics	Accorde l'autorisation d'obtenir des métriques	Lecture			
GetMulticastGroup	Accorde l'autorisation d'obtenir le MulticastGroup	Lecture	MulticastGroup*		
GetMulticastGroupSession	Accorde l'autorisation d'accéder à la MulticastGroup session	Lecture	MulticastGroup*		
GetNetworkAnalyzerConfiguration	Accorde l'autorisation d'obtenir le NetworkAnalyzerConfiguration	Lecture	NetworkAnalyzerConfiguration*		
GetPartnerAccount	Accorde l'autorisation d'obtenir les informations associées PartnerAccount	Lecture	SidewalkAccount*		
GetPosition	Accorde l'autorisation d'obtenir la position d'une ressource donnée	Lecture	WirelessDevice		
			WirelessGateway		
GetPositionConfiguration	Accorde l'autorisation d'obtenir la configuration de la position d'une ressource donnée	Lecture	WirelessDevice		
			WirelessGateway		
GetPositionEstimate	Accorde l'autorisation d'obtenir une estimation d'emplacement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourceEventConfiguration	Accorde l'autorisation d'obtenir une configuration d'événement pour un identifiant	Lecture	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
GetResourceLogLevel	Accorde l'autorisation d'obtenir un niveau de journal de ressource	Lecture	WirelessDevice		
			WirelessGateway		
GetResourcePosition	Accorde l'autorisation d'obtenir la position d'une ressource donnée	Lecture	WirelessDevice		
			WirelessGateway		
GetServiceEndpoint	Accorde l'autorisation de récupérer le point de terminaison spécifique au compte client pour la connexion au protocole CUPS ou au protocole LoRa WAN Network Server (LNS), et éventuellement le certificat de confiance du serveur au format PEM	Lecture			
GetServiceProfile	Accorde l'autorisation d'obtenir le ServiceProfile	Lecture	ServiceProfile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWirelessDevice	Accorde l'autorisation d'obtenir le WirelessDevice	Lecture	WirelessDevice*		
GetWirelessDeviceImportTask	Octroie l'autorisation d'obtenir la tâche d'importation de périphériques sans fil	Lecture	ImportTask*		
GetWirelessDeviceStatistics	Accorde l'autorisation d'obtenir des informations statistiques pour une donnée WirelessDevice	Lecture	WirelessDevice*		
GetWirelessGateway	Accorde l'autorisation d'obtenir le WirelessGateway	Lecture	WirelessGateway*		
GetWirelessGatewayCertificate	Accorde l'autorisation d'obtenir l'identifiant du certificat IoT Core Identity associé au WirelessGateway	Lecture	WirelessGateway*		
GetWirelessGatewayFirmwareInformation	Octroie l'autorisation d'obtenir la version actuelle du microprogramme et d'autres informations relatives au WirelessGateway	Lecture	WirelessGateway*		
GetWirelessGatewayStatistics	Accorde l'autorisation d'obtenir des informations statistiques pour une donnée WirelessGateway	Lecture	WirelessGateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWirelessGatewayTask	Accorde l'autorisation d'obtenir la tâche pour une tâche donnée WirelessGateway	Lecture	WirelessGateway*		
GetWirelessGatewayTaskDefinition	Accorde l'autorisation d'obtenir la définition de WirelessGateway tâche donnée	Lecture	WirelessGatewayTaskDefinition*		
ListDestinations	Accorde l'autorisation de répertorier les informations des destinations disponibles sur la base du Compte AWS	Lecture			
ListDeviceProfiles	Octroie l'autorisation de répertorier les informations disponibles sur la DevicePro files base du Compte AWS	Lecture			
ListDevicesForWirelessDeviceImportTask	Accorde l'autorisation de répertorier les informations des appareils par tâche d'importation d'appareils sans fil sur la base de Compte AWS	Lecture	ImportTask*		
ListEventConfigurations	Accorde l'autorisation de répertorier les informations relatives aux configurations d'événements disponibles sur la base du Compte AWS	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFuotaTasks	Octroie l'autorisation de répertorier les informations disponibles sur la FuotaTasks base du Compte AWS	Lecture			
ListMulticastGroups	Octroie l'autorisation de répertorier les informations disponibles sur la Multicast Groups base du Compte AWS	Lecture			
ListMulticastGroupsByFuotaTask	Octroie l'autorisation de répertorier les informations disponibles MulticastGroups sur la FuotaTask base du Compte AWS	Lecture	FuotaTask *		
ListNetworkAnalyzerConfigurations	Octroie l'autorisation de répertorier les informations disponibles sur la NetworkAnalyzerConfigurations base du Compte AWS	Lecture			
ListPartnerAccounts	Accorde l'autorisation de répertorier les comptes partenaires disponibles	Lecture			
ListPositionConfigurations	Accorde l'autorisation de répertorier les informations relatives aux configurations de position disponibles sur la base de Compte AWS	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListQueuedMessages	Accorde l'autorisation de répertorier les messages mis en file d'attente	Lecture			
ListServiceProfiles	Octroie l'autorisation de répertorier les informations disponibles sur la ServicePr ofiles base du Compte AWS	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les identifications d'une ressource donnée.	Lecture	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
ListWirelessDeviceImportTasks	Accorde l'autorisation de répertorier les informations relatives aux tâches d'importation de périphériques sans fil sur la base du Compte AWS	Lecture			
ListWirelessDevices	Octroie l'autorisation de répertorier les informations disponibles sur la WirelessDevices base du Compte AWS	Lecture			
ListWirelessGatewayTaskDefinitions	Accorde l'autorisation de répertorier les informations relatives aux définitions de WirelessGateway tâches disponibles sur la base de Compte AWS	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWirelessGateways	Octroie l'autorisation de répertorier les informations disponibles sur la WirelessGateways base du Compte AWS	Lecture			
PutPositionConfiguration	Accorde l'autorisation d'établir la configuration de position pour une ressource donnée	Écrire	WirelessDevice		
			WirelessGateway		
PutResourceLogLevel	Accorde l'autorisation de placer un niveau de journal de ressource	Écriture	WirelessDevice		
			WirelessGateway		
ResetAllResourceLogLevels	Accorde l'autorisation de réinitialiser tous les niveaux de journal de ressource	Écriture			
ResetResourceLogLevel	Accorde l'autorisation de réinitialiser un niveau de journal de ressource.	Écrire	WirelessDevice		
			WirelessGateway		
SendDataToMulticastGroup	Accorde l'autorisation d'envoyer des données à MulticastGroup	Écrire	MulticastGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendDataToWirelessDevice	Accorde l'autorisation d'envoyer le cadre de données d'application déchiffré au périphérique cible.	Écrire	WirelessDevice*		
StartBulkAssociateWirelessDeviceWithMulticastGroup	Accorde l'autorisation de les WirelessDevices associer à MulticastGroup	Écrire	MulticastGroup*		
StartBulkDisassociateWirelessDeviceFromMulticastGroup	Accorde l'autorisation de dissocier en bloc le WirelessDevices MulticastGroup	Écrire	MulticastGroup*		
StartFuotaTask	Accorde l'autorisation de démarrer le FuotaTask	Écrire	FuotaTask*		
StartMulticastGroupSession	Accorde l'autorisation de démarrer la MulticastGroup session	Écrire	MulticastGroup*		
StartNetworkAnalyzerStream	Accorde l'autorisation de démarrer le NetworkAnalyzer stream	Écrire	NetworkAnalyzerConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartSingleWirelessDeviceImportTask	Octroie l'autorisation de lancer l'unique tâche d'importation de périphériques sans fil	Écrire	Destination		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartWirelessDeviceImportTask	Octroie l'autorisation de lancer la tâche d'importation de périphériques sans fil	Écrire	ImportTask*		
			Destination		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation de baliser une ressource donnée.	Balisage	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestWirelessDevice	Accorde l'autorisation de simuler un appareil mis en service pour envoyer des données de liaison montante avec la charge utile 'Hello'.	Écriture	WirelessDevice*		
UntagResource	Accorde l'autorisation de supprimer les balises données de la ressource.	Balisage	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:TagKeys	
UpdateDestination	Accorde l'autorisation de mettre à jour une ressource Destination.	Écrire	Destination*		
UpdateEventConfigurationByResourceTypes	Accorde l'autorisation de mettre à jour la configuration d'événements par types de ressources	Écrire			
UpdateFuotaTask	Accorde l'autorisation de mettre à jour le FuotaTask	Écrire	FuotaTask*		
UpdateLogLevelsByResourceTypes	Accorde l'autorisation de mettre à jour les niveaux de journal par type de ressource	Écrire			
UpdateMetricConfiguration	Accorde l'autorisation de mettre à jour la configuration des métriques	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMulticastGroup	Accorde l'autorisation de mettre à jour le MulticastGroup	Écrire	MulticastGroup*		
UpdateNetworkAnalyzerConfiguration	Accorde l'autorisation de mettre à jour le NetworkAnalyzerConfiguration	Écrire	MulticastGroup*		
			NetworkAnalyzerConfiguration*		
			WirelessDevice*		
			WirelessGateway*		
UpdatePartnerAccount	Accorde l'autorisation de mettre à jour un compte partenaire.	Écrire	SidewalkAccount*		
UpdatePosition	Accorde l'autorisation de mettre à jour la position d'une ressource donnée	Écrire	WirelessDevice		
			WirelessGateway		
UpdateResourceEventConfiguration	Accorde l'autorisation de mettre à jour la configuration d'un événement pour un identifiant	Écrire	SidewalkAccount		
			WirelessDevice		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			WirelessGateway		
UpdateResourcePosition	Accorde l'autorisation de mettre à jour la position d'une ressource donnée	Écrire	WirelessDevice		
			WirelessGateway		
UpdateWirelessDevice	Autorise la mise à jour d'une WirelessDevice ressource	Écrire	WirelessDevice*		
			Destination		
			DeviceProfile		
			ServiceProfile		
UpdateWirelessDeviceImportTask	Octroie l'autorisation de mettre à jour une tâche d'importation de périphériques sans fil	Écrire	ImportTask*		
UpdateWirelessGateway	Autorise la mise à jour d'une WirelessGateway ressource	Écrire	WirelessGateway*		

Types de ressources définis par AWS IoT Wireless

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
WirelessDevice	`arn:${Partition}:iotwireless:${Region}:${Account}:WirelessDevice/${WirelessDeviceId}`	aws:ResourceTag/${TagKey}
WirelessGateway	`arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGateway/${WirelessGatewayId}`	aws:ResourceTag/${TagKey}
DeviceProfile	`arn:${Partition}:iotwireless:${Region}:${Account}:DeviceProfile/${DeviceProfileId}`	aws:ResourceTag/${TagKey}
ServiceProfile	`arn:${Partition}:iotwireless:${Region}:${Account}:ServiceProfile/${ServiceProfileId}`	aws:ResourceTag/${TagKey}
Destination	`arn:${Partition}:iotwireless:${Region}:${Account}:Destination/${DestinationName}`	aws:ResourceTag/${TagKey}
SidewalkAccount	`arn:${Partition}:iotwireless:${Region}:${Account}:SidewalkAccount/${SidewalkAccountId}`	aws:ResourceTag/${TagKey}
WirelessGatewayTaskDefinition	`arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGatewayTaskDef`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
	inition/${WirelessGatewayTaskDefinitionId}	
FuotaTask	arn:${Partition}:iotwireless:${Region}:${Account}:FuotaTask/${FuotaTaskId}	aws:ResourceTag/${TagKey}
Multicast Group	arn:${Partition}:iotwireless:${Region}:${Account}:MulticastGroup/${MulticastGroupId}	aws:ResourceTag/${TagKey}
NetworkAnalyzerConfiguration	arn:${Partition}:iotwireless:${Region}:${Account}:NetworkAnalyzerConfiguration/${NetworkAnalyzerConfigurationName}	aws:ResourceTag/${TagKey}
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
cert	arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}	
ImportTask	arn:${Partition}:iotwireless:${Region}:${Account}:ImportTask/${ImportTaskId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS IoT Wireless

AWS IoT Wireless définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'une clé de balise présente dans la demande envoyée par l'utilisateur à la ressource IoT Wireless.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction d'un composant de clé de balise d'une balise attachée à une ressource IoT Wireless.	String
aws:TagKeys	Filtre l'accès en fonction de la liste de tous les noms de clés de balise associés à la ressource dans la demande	ArrayOfString
iotwireless:DestinationName	Filtre l'accès par nom de destination associé à la ressource IoT Wireless	String
iotwireless:DeviceProfileId	Filtre l'accès par identifiant de profil d'appareil associé à la ressource IoT Wireless	String
iotwireless:ServiceProfileId	Filtre l'accès par identifiant de profil de service associé à la ressource IoT Wireless	String

Actions, ressources et clés de condition pour AWS IQ

AWS IQ (préfixe de service :`iq`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IQ
- Types de ressources définis par AWS IQ
- Clés de condition pour AWS IQ

Actions définies par AWS IQ

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptCall	Accorde l'autorisation d'accepter un voice/video appel entrant	Écrire	call*		
ApprovePaymentRequest	Accorde l'autorisation d'approuver une demande de paiement	Écrire	paymentRequest*		
ApproveProposal	Accorde l'autorisation d'approuver une proposition	Écrire	proposal*		
ArchiveConversation	Accorde l'autorisation d'archiver une conversation	Écrire	conversation*		
CompleteProposal	Accorde l'autorisation de terminer une proposition	Écrire	proposal*		
CreateConversation	Autorise à répondre à une demande ou à envoyer un message direct pour lancer une conversation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExpert	Accorde l'autorisation de créer un profil d'expert	Écrire			
CreateListing	Accorde l'autorisation de créer une liste	Écrire			
CreateMilestoneProposal	Accorde l'autorisation de créer une proposition d'étape	Écrire			
CreatePaymentRequest	Accorde l'autorisation de créer une demande de paiement	Écrire			
CreateProject	Accorde l'autorisation de soumettre de nouvelles demandes	Écrire			
CreateRequest	Accorde l'autorisation de soumettre de nouvelles demandes	Écrire			
CreateScheduledProposal	Accorde l'autorisation de créer une proposition planifiée	Écrire			
CreateSeller	Accorde l'autorisation de créer un profil de vendeur	Écrire			
CreateUpfrontProposal	Accorde l'autorisation de créer une proposition initiale	Écrire			
DeclineCall	Autorise le refus d'un voice/video appel entrant	Écrire	call*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAttachment	Accorde l'autorisation de supprimer une pièce jointe existante	Écrire	attachment*		
DisableIndividualPublicProfile	Accorde l'autorisation de désactiver une page de profil public individuelle	Écrire	expert*		
DownloadAttachment	Accorde l'autorisation de télécharger une pièce jointe existante.	Lecture	attachment*		
EnableIndividualPublicProfile	Accorde l'autorisation d'activer une page de profil public individuelle	Écrire	expert*		
EndCall	Accorde l'autorisation de mettre fin à un voice/video appel	Écrire	call*		
GetBuyer	Accorde l'autorisation de lire les informations relatives à l'acheteur	Lecture	buyer*		
GetCall	Autorise la lecture des détails d'un voice/video appel	Lecture	call*		
GetChatInfo	Accorde l'autorisation de lire les détails de l'environnement de discussion à propos d'une conversation	Lecture	conversation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetChatMessages	Accorder l'autorisation de lire les messages de discussion dans une conversation	Lecture	conversation*		
GetChatToken	Accorde l'autorisation de demander un jeton websocket pour les notifications de conversation	Lecture	token*		
GetCompanyChatMessages	Accorde l'autorisation de lire les messages instantanés dans une conversation au sein de l'entreprise	Lecture	conversation*		
GetCompanyProfile	Accorder l'autorisation de lire un profil d'entreprise	Lecture	company*		
GetConversation	Accorde l'autorisation de lire les détails d'une conversation	Lecture	conversation*		
GetExpert	Accorde l'autorisation de lire les informations relatives à l'expert	Lecture	expert*		
GetListing	Accorde l'autorisation de lire une liste	Lecture	listing*		
GetMarketplaceSeller	Accorde l'autorisation de lire les informations d'un profil de vendeur	Lecture	seller*		
GetPaymentRequest	Accorde l'autorisation de lire une demande de paiement	Lecture	paymentRequest*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProposal	Accorde l'autorisation de lire une proposition	Lecture	proposal*		
GetRequest	Accorde l'autorisation d'obtenir une demande créée.	Lecture	request*		
GetReview	Accorder l'autorisation de lire un avis pour un expert	Lecture	seller*		
HideRequest	Accorde l'autorisation de masquer une demande	Écrire	request*		
InitiateCall	Accorde l'autorisation de démarrer un voice/video appel	Écrire			
LinkAwsCertification	Permet de lier une AWS certification à un profil individuel	Écrire	expert*		
ListAttachments	Accorde l'autorisation de répertorier les pièces jointes existantes.	List	attachment*		
ListConversations	Accorde l'autorisation de répertorier les conversations existantes	Lecture	conversation*		
ListExpertAccessLogs	Accorde l'autorisation de répertorier les journaux d'accès des activités des experts	Lecture	permission*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListListings	Accorde l'autorisation d'établir des listes	Lecture	listing*		
ListPaymentRequests	Accorde l'autorisation de répertorier les demandes de paiement	Lecture	paymentRequest		
			paymentSchedule		
ListProposals	Accorde l'autorisation de répertorier les propositions	Lecture	proposal*		
ListRequests	Accorde l'autorisation de répertorier les demandes qui sont créées	Lecture	request*		
ListReviews	Accorder l'autorisation de répertorier les avis d'un expert	Lecture	seller*		
MarkChatMessageRead	Accorder la permission de marquer un message comme lu dans une conversation	Écrire	conversation*		
RejectPaymentRequest	Accorde l'autorisation de rejeter une demande de paiement	Écrire	paymentRequest*		
RejectProposal	Accorde l'autorisation de rejeter une proposition	Écrire	proposal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendCompanyChatMessage	Accorde l'autorisation d'envoyer un message dans une conversation en tant qu'entreprise	Écrire	conversation*		
SendIndividualChatMessage	Accorde l'autorisation d'envoyer un message dans une conversation en tant qu'individu	Écrire	conversation*		
UnarchiveConversation	Accorde l'autorisation de désarchiver une conversation	Écrire	conversation*		
UnlinkAwsCertification	Accorde l'autorisation de dissocier une AWS certification du profil individuel	Écrire	expert*		
UpdateCompanyProfile	Accorde l'autorisation de mettre à jour un profil d'entreprise	Écrire	company*		
UpdateConversationMembers	Accorder l'autorisation d'ajouter d'autres participants à une conversation	Écrire	conversation*		
UpdateExpert	Accorde l'autorisation de mettre à jour les informations d'un expert	Écrire	expert*		
UpdateListing	Accorde l'autorisation de mettre à jour une liste	Écrire	listing*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRequest	Accorde l'autorisation de mettre à jour une demande	Écrire	request*		
UploadAttachment	Accorde l'autorisation de télécharger une pièce jointe	Écrire			
WithdrawPaymentRequest	Accorde l'autorisation de retirer une demande de paiement	Écrire	paymentRequest*		
WithdrawProposal	Accorde l'autorisation de retirer une proposition	Écrire	proposal*		
WriteReview	Accorder l'autorisation de rédiger un avis pour un expert	Écrire	seller*		

Types de ressources définis par AWS IQ

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
conversation	`arn:${Partition}:iq:${Region}::conversation/${ConversationId}`	

Types de ressources	ARN	Clés de condition
buyer	arn:${Partition}:iq:${Region}::buyer/${BuyerId}	
expert	arn:${Partition}:iq:${Region}::expert/${ExpertId}	
call	arn:${Partition}:iq:${Region}::call/${CallId}	
token	arn:${Partition}:iq:${Region}::token/${TokenId}	
proposal	arn:${Partition}:iq:${Region}::proposal/${ConversationId}/${ProposalId}	
paymentRequest	arn:${Partition}:iq:${Region}::paymentRequest/${ConversationId}/${ProposalId}/${PaymentRequestId}	
paymentSchedule	arn:${Partition}:iq:${Region}::paymentSchedule/${ConversationId}/${ProposalId}/${VersionId}	
seller	arn:${Partition}:iq:${Region}::seller/${SellerAwsAccountId}	
company	arn:${Partition}:iq:${Region}::company/${CompanyId}	
request	arn:${Partition}:iq:${Region}::request/${RequestId}	
listing	arn:${Partition}:iq:${Region}::listing/${ListingId}	

Types de ressources	ARN	Clés de condition
attachment	`arn:${Partition}:iq:${Region}::attachment/${AttachmentId}`	
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Clés de condition pour AWS IQ

IQ ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS IQ Permissions

AWS IQ Permissions (préfixe de service :`iq-permission`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS IQ Permissions
- Types de ressources définis par AWS IQ Permissions
- Clés de condition pour les autorisations AWS IQ

Actions définies par AWS IQ Permissions

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApproveAccessGrant	Accorde l'autorisation d'approuver une demande d'autorisation	Écrire	permission*		
ApprovePermissionRequest	Accorde l'autorisation d'approuver une demande d'autorisation	Écrire	permission*		
AssumePermissionRole	Accorde l'autorisation d'obtenir un ensemble d'informations de sécurité temporaires pour les experts, qu'ils peuvent utiliser pour accéder aux ressources des acheteurs AWS	Écrire	permission*		
CreatePermissionRequest	Accorde l'autorisation de créer une demande de parc d'instances Spot.	Écrire	permission*		
GetPermissionRequest	Accorde l'autorisation d'obtenir une demande d'autorisation	Lecture	permission*		
ListPermissionRequests	Accorde l'autorisation de répertorier les demandes d'autorisation	Lecture	permission*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RejectPermissionRequest	Accorde l'autorisation de rejeter la demande d'annexe	Écrire	permission*		
RevokePermissionRequest	Accorde l'autorisation de révoquer une demande d'autorisation qui a été précédemment approuvée	Écrire	permission*		
WithdrawPermissionRequest	Autorise le retrait d'une demande d'autorisation qui n'a pas été approuvée ou refusée	Écrire	permission*		

Types de ressources définis par AWS IQ Permissions

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Clés de condition pour les autorisations AWS IQ

IQ Permission ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Kendra

Amazon Kendra (préfixe de service : `kendra`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Kendra
- Types de ressources définis par Amazon Kendra
- Clés de condition pour Amazon Kendra

Actions définies par Amazon Kendra

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateEntitiesToExperience	Accorde l'autorisation de placer le mappage principal dans l'index	Écrire	experience*		
			index*		
AssociatePersonasToEntities	Définit les autorisations spécifiques des utilisateurs ou des groupes dans votre source d'identité AWS SSO avec accès à votre expérience Amazon Kendra	Écrire	experience*		
			index*		
BatchDeleteDocument	Accorde l'autorisation de supprimer des documents par lots	Écrire	index*		
BatchDeleteFeaturedResultsSet	Accorde l'autorisation de supprimer un jeu de résultats présenté	Écrire	featured-results-set*		
			index*		
BatchGetDocumentStatus	Accorde l'autorisation d'obtenir par lots le statut de document	Lecture	index*		
BatchPutDocument	Accorde l'autorisation d'ajouter des documents par lots	Écrire	index*		
ClearQuerySuggestions	Accorde l'autorisation d'effacer les suggestions pour un	Écrire	index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	index donné généré jusqu'à maintenant				
CreateAccessControlConfiguration	Accorde l'autorisation de créer une configuration de contrôle d'accès	Écrire	index*		
CreateDataSource	Accorde l'autorisation de créer une source de données.	Écrire	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExperience	Crée une expérience Amazon Kendra, telle qu'une application de recherche	Écrire	index*		
CreateFaq	Accorde l'autorisation de créer une FAQ	Écrire	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeaturedResultsSet	Accorde l'autorisation de créer un jeu de résultats présenté	Écrire	index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Accorde l'autorisation de créer un index	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuerySuggestionsBlockList	Accorde l'autorisation de créer un QuerySuggestions BlockList	Écrire	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThesaurus	Accorde l'autorisation de créer un thésaurus	Écrire	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccessControlConfiguration	Accorde l'autorisation de supprimer une configuration de contrôle d'accès	Écrire	access-control-configuration*		
			index*		
DeleteDataSource	Accorde l'autorisation de supprimer une source de données.	Écrire	data-source*		
			index*		
DeleteExperience	Supprime votre expérience Amazon Kendra, telle qu'une application de recherche	Écrire	experience*		
			index*		
DeleteFaq	Accorde l'autorisation de supprimer une FAQ	Écrire	faq*		
			index*		
DeleteIndex	Accorde l'autorisation de supprimer un index	Écrire	index*		
DeletePrincipalMapping	Accorde l'autorisation de supprimer le mappage principal de l'index	Écrire	index*		
			data-source		
DeleteQuerySuggestionsBlockList	Accorde l'autorisation de supprimer un QuerySuggestions BlockList	Écrire	index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			query-suggestions-block-list*		
DeleteThesaurus	Accorde l'autorisation de supprimer un thésaurus	Écrire	index*		
			thesaurus*		
DescribeAccessControlConfiguration	Accorde l'autorisation de décrire une configuration de contrôle d'accès	Lecture	access-control-configuration*		
			index*		
DescribeDataSource	Accorde l'autorisation de décrire une source de données	Lecture	data-source*		
			index*		
DescribeExperience	Obtient des informations sur votre expérience Amazon Kendra, comme une application de recherche	Lecture	experience*		
			index*		
DescribeFaq	Accorde l'autorisation de décrire une FAQ	Lecture	faq*		
			index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFeaturedResultsSet	Accorde l'autorisation de décrire un jeu de résultats présenté	Lecture	featured-results-set*		
			index*		
DescribeIndex	Accorde l'autorisation de décrire un index	Lecture	index*		
DescribePrincipalMapping	Accorde l'autorisation de décrire le mappage principal depuis l'index	Lecture	index*		
			data-source		
DescribeQuerySuggestionsBlockList	Accorde l'autorisation de décrire un QuerySuggestions BlockList	Lecture	index*		
			query-suggestions-block-list*		
DescribeQuerySuggestionsConfig	Accorde l'autorisation de décrire la configuration des suggestions de requête pour un index	Lecture	index*		
DescribeThesaurus	Accorde l'autorisation de décrire un thésaurus	Lecture	index*		
			thesaurus*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateEntitiesFromExperience	Empêche les utilisateurs ou les groupes de votre source d'identité AWS SSO d'accéder à votre expérience Amazon Kendra	Écrire	experience*		
			index*		
DisassociatePersonasFromEntities	Supprime les autorisations spécifiques des utilisateurs ou des groupes de votre source d'identité AWS SSO avec accès à votre expérience Amazon Kendra	Écrire	experience*		
			index*		
GetQuerySuggestions	Accorde l'autorisation d'obtenir des suggestions pour un préfixe de requête	Lecture	index*		
GetSnapshots	Récupère les données des métriques de recherche	Lecture	index*		
ListAccessControlConfigurations	Accorde l'autorisation de répertorier les configurations de contrôle d'accès	List	index*		
ListDataSourceSyncJobs	Accorde l'autorisation d'obtenir l'historique des tâches de synchronisation des sources de données	List	data-source*		
			index*		
ListDataSources	Accorde l'autorisation de répertorier les sources de données	List	index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEntityPersonas	Répertorie les autorisations spécifiques des utilisateurs et des groupes ayant accès à votre expérience Amazon Kendra	List	experience*		
			index*		
ListExperienceEntities	Répertorie les utilisateurs ou les groupes de votre source d'identité AWS SSO autorisés à accéder à votre expérience Amazon Kendra	List	experience*		
			index*		
ListExperiences	Répertorie une ou plusieurs expériences Amazon Kendra. Vous pouvez créer une expérience Amazon Kendra, telle qu'une application de recherche	List	index*		
ListFaqs	Accorde l'autorisation de répertorier les FAQ	List	index*		
ListFeaturedResultsSets	Accorde l'autorisation de répertorier les jeux de résultats présentés	List	index*		
ListGroupsOlderThanOrderingId	Accorde l'autorisation de répertorier les groupes plus anciens qu'un ID de classement	List	index*		
			data-source		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIndices	Accorde l'autorisation de répertorier les index	List			
ListQuerySuggestionsBlockLists	Accorde l'autorisation de répertorier les QuerySuggestions BlockLists	List	index*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
ListThesauri	Accorde l'autorisation de répertorier des thésaurus	List	index*		
PutPrincipalMapping	Accorde l'autorisation de placer le mappage principal dans l'index	Écrire	index*		
			data-source		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Query	Accorde l'autorisation d'interroger des documents et des FAQ	Lecture	index*		
Retrieve	Accorde l'autorisation de récupérer le contenu pertinent d'un index	Lecture	index*		
StartDataSourceSyncJob	Accorde l'autorisation de démarrer la tâche de synchronisation des sources de données	Écrire	data-source*		
			index*		
StopDataSourceSyncJob	Accorde l'autorisation d'arrêter la tâche de synchronisation des sources de données	Écrire	data-source*		
			index*		
SubmitFeedback	Accorde l'autorisation d'envoyer des commentaires sur les résultats d'une requête	Écrire	index*		
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Identification	data-source		
			faq		
			featured-results-set		
			index		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			query-suggestions-block-list		
			thesaurus		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer la balise avec la clé donnée d'une ressource	Identification	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateAccessControlConfiguration	Accorde l'autorisation de mettre à jour une configuration de contrôle d'accès	Écrire	access-control-configuration*		
			index*		
UpdateDataSource	Accorde l'autorisation de mettre à jour une source de données	Écrire	data-source*		
			index*		
UpdateExperience	Met à jour votre expérience Amazon Kendra, telle qu'une application de recherche	Écrire	index*		
UpdateFeaturedResultsSet	Accorde l'autorisation de mettre à jour un jeu de résultats présenté	Écrire	featured-results-set*		
			index*		
UpdateIndex	Accorde l'autorisation de mettre à jour un index	Écrire	index*		
UpdateQuerySuggestionsBlockList	Accorde l'autorisation de mettre à jour un QuerySuggestions BlockList	Écrire	index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			query-suggestions-block-list*		
UpdateQuerySuggestionsConfig	Accorde l'autorisation de mettre à jour la configuration des suggestions de requête pour un index	Écrire	index*		
UpdateThesaurus	Accorde l'autorisation de mettre à jour un thésaurus	Écrire	index*		
			thesaurus*		

Types de ressources définis par Amazon Kendra

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
index	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
data-source	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/data-source/${DataSourceId}	aws:ResourceTag/${TagKey}
faq	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/faq/${FaqId}	aws:ResourceTag/${TagKey}
experience	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/experience/${ExperienceId}	
thesaurus	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/thesaurus/${ThesaurusId}	aws:ResourceTag/${TagKey}
query-suggestions-block-list	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/query-suggestions-block-list/${QuerySuggestionsBlockListId}	aws:ResourceTag/${TagKey}
featured-results-set	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/featured-results-set/${FeaturedResultsSetId}	aws:ResourceTag/${TagKey}
access-control-configuration	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/access-control-configuration/${AccessControlConfigurationId}	

Clés de condition pour Amazon Kendra

Amazon Kendra définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking (préfixe de service : `kendra-ranking`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Kendra Intelligent Ranking
- Types de ressources définis par Amazon Kendra Intelligent Ranking
- Clés de condition pour Amazon Kendra Intelligent Ranking

Actions définies par Amazon Kendra Intelligent Ranking

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRescoreExecutionPlan	Accorde l'autorisation de créer un RescoreExecutionPlan	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRescoreExecutionPlan	Accorde l'autorisation de supprimer un RescoreExecutionPlan	Écrire	rescore-execution-plan*		
DescribeRescoreExecutionPlan	Accorde l'autorisation de décrire un RescoreExecutionPlan	Lecture	rescore-execution-plan*		
ListRescoreExecutionPlans	Accorde l'autorisation de tout répertorier RescoreExecutionPlans	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	rescore-execution-plan		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Rescore	Accorde l'autorisation de réévaluer les documents avec Kendra Intelligent Ranking	Lecture	rescore-execution-plan*		
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Identification	rescore-execution-plan		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer la balise avec la clé donnée d'une ressource	Identification	rescore-execution-plan		
				aws:TagKeys	
UpdateRescoreExecutionPlan	Accorde l'autorisation de mettre à jour un RescoreExecutionPlan	Écrire	rescore-execution-plan*		

Types de ressources définis par Amazon Kendra Intelligent Ranking

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
rescore-execution-plan	`arn:${Partition}:kendra-ranking:${Region}:${Account}:rescore-execution-plan/${RescoreExecutionPlanId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) (préfixe de service : `cassandra`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Keyspaces (for Apache Cassandra)
- Types de ressources définis par Amazon Keyspaces (for Apache Cassandra)
- Clés de condition pour Amazon Keyspaces (for Apache Cassandra)

Actions définies par Amazon Keyspaces (for Apache Cassandra)

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Alter	Accorde l'autorisation de modifier un espace de clés ou une table	Écrire	keyspace		
			table		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
AlterMultiRegionResource	Accorde l'autorisation de modifier un espace de clés ou une table multirégion	Écrire	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Create	Accorde l'autorisation de créer un espace de clés ou une table	Écrire	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiRegionResource	Accorde l'autorisation de créer un espace de clés ou une table multirégion	Écrire	keyspace		
			table		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
Drop	Accorde l'autorisation de supprimer un espace de clés ou une table	Écrire	keyspace		
			table		
DropMultiRegionResource	Accorde l'autorisation de supprimer un espace de clés ou une table multirégion	Écrire	keyspace		
			table		
GetRecords	Accorde l'autorisation de récupérer les enregistrements du flux CDC à partir d'une partition donnée	Lecture	stream*		
GetShardIterator	Accorde l'autorisation de renvoyer un itérateur de partition	Lecture	stream*		
GetStream	Accorde l'autorisation de renvoyer des informations sur un flux CDC, y compris la composition de ses fragments	Lecture	stream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStreams	Autorise le renvoi d'un tableau de flux CDC ARNs associés au compte courant et au point de terminaison	List			
Modify	Accorde l'autorisation d'accès aux données INSERT, UPDATE ou DELETE dans une table	Écrire	table*		
ModifyMultiRegionResource	Accorde l'autorisation d'accès aux données INSERT, UPDATE ou DELETE dans une table multirégion	Écrire	table*		
Restore	Accorde l'autorisation de restaurer une table à partir d'une sauvegarde	Écrire	table*		
RestoreMultiRegionTable	Accorde l'autorisation de restaurer une table multirégion à partir d'une sauvegarde	Écrire	table*		
Select	Accorde l'autorisation d'accès aux données SELECT d'une table	Lecture	table*		
SelectMultiRegionResource	Accorde l'autorisation d'accès aux données SELECT d'une table multirégion	Lecture	table*		
		Identification	keyspace		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagMultiRegionResource	Accorde l'autorisation de baliser un espace de clés ou une table multirégion		table		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation de baliser un keyspace, une table ou un flux	Identification	keyspace		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagMultiRegionResource	Accorde l'autorisation d'annuler le balisage d'un espace de clés ou d'une table multirégion	Identification	keyspace		
			table		
				aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer le balisage d'un keyspace, d'une table ou d'un flux	Identification	keyspace		
			stream		
			table		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdatePartitioner	Accorde l'autorisation de METTRE À JOUR le partitionneur dans une table système	Écrire	table*		

Types de ressources définis par Amazon Keyspaces (for Apache Cassandra)

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
keyspace	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}/stream/${StreamLabel}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (pour Apache Cassandra) définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Kinesis Analytics

Amazon Kinesis Analytics (préfixe de service : `kinesisanalytics`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Kinesis Analytics

- Types de ressources définis par Amazon Kinesis Analytics
- Clés de condition pour Amazon Kinesis Analytics

Actions définies par Amazon Kinesis Analytics

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddApplicationInput	Accorde l'autorisation d'ajouter des entrées à l'application	Écrire	application*		
AddApplicationOutput	Accorde l'autorisation d'ajouter des sorties à l'application	Écriture	application*		
AddApplicationReferenceDataSource	Accorde l'autorisation d'ajouter une source de données de référence à l'application	Écrire	application*		
CreateApplication	Accorde l'autorisation de créer une application	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteApplicationOutput	Accorde l'autorisation de supprimer la sortie spécifiée de l'application	Écriture	application*		
DeleteApplicationReferenceDataSource	Accorde l'autorisation de supprimer la source de données de référence spécifiée de l'application	Écrire	application*		
DescribeApplication	Accorde l'autorisation de décrire l'application spécifiée	Lecture	application*		
DiscoverInputSchema	Accorde l'autorisation de découvrir le schéma d'entrée pour l'application	Lecture			
GetApplicationState [autorisation uniquement]	Accorde à la console Kinesis Data Analytics l'autorisation d'afficher les résultats de flux pour les applications d'exécution SQL Kinesis Data Analytics	Lecture	application*		
ListApplications	Accorde l'autorisation de répertorier des demandes pour le compte	Liste			
ListTagsForResource	Accorde l'autorisation de récupérer les balises associées à l'application	Lecture	application*		
StartApplication	Accorde l'autorisation de démarrer l'application	Écriture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopApplication	Accorde l'autorisation d'arrêter l'application	Écriture	application*		
TagResource	Accorde l'autorisation d'ajouter des balises à l'application	Balisage	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de l'application	Balisage	application*		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour l'application	Écrire	application*		

Types de ressources définis par Amazon Kinesis Analytics

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Kinesis Analytics

Amazon Kinesis Analytics définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'un ensemble de valeurs pour chacune des étiquettes	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Kinesis Analytics V2

Amazon Kinesis Analytics V2 (préfixe de service : `kinesisanalytics`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Kinesis Analytics V2
- Types de ressources définis par Amazon Kinesis Analytics V2
- Clés de condition pour Amazon Kinesis Analytics V2

Actions définies par Amazon Kinesis Analytics V2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddApplicationCloudWatchLoggingOption	Accorde l'autorisation d'ajouter l'option de journalisation CloudWatch à l'application	Écriture	application*		
AddApplicationInput	Accorde l'autorisation d'ajouter des entrées à l'application	Écriture	application*		
AddApplicationInputProcessi	Accorde l'autorisation d'ajouter une configuration de traitement des entrées à l'application	Écriture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ngConfiguration					
AddApplicationOutput	Accorde l'autorisation d'ajouter des sorties à l'application	Écriture	application*		
AddApplicationReferenceDataSource	Accorde l'autorisation d'ajouter une source de données de référence à l'application	Écriture	application*		
AddApplicationVpcConfiguration	Accorde l'autorisation d'ajouter une configuration VPC à l'application	Écriture	application*		
CreateApplication	Accorde l'autorisation de créer une application	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateApplicationPresignedUrl	Accorde l'autorisation de créer et de renvoyer une URL que vous pouvez utiliser pour vous connecter à l'extension d'une application	Lecture	application*		
CreateApplicationSnapshot	Accorde l'autorisation de créer un instantané pour une application	Écriture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteApplication	Accorde l'autorisation de supprimer une application	Écriture	application*		
DeleteApplicationCloudWatchLoggingOption	Accorde l'autorisation de supprimer l'option de journalisation CloudWatch spécifiée de l'application	Écriture	application*		
DeleteApplicationInputProcessingConfiguration	Accorde l'autorisation de supprimer la configuration de traitement des entrées spécifiée de l'application	Écriture	application*		
DeleteApplicationOutput	Accorde l'autorisation de supprimer la sortie spécifiée de l'application	Écriture	application*		
DeleteApplicationReferenceDataSource	Accorde l'autorisation de supprimer la source de données de référence spécifiée de l'application	Écriture	application*		
DeleteApplicationSnapshot	Accorde l'autorisation de supprimer un instantané pour une application	Écriture	application*		
DeleteApplicationVpcConfiguration	Accorde l'autorisation de supprimer la configuration VPC spécifiée de l'application	Écriture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeApplication	Accorde l'autorisation de décrire l'application spécifiée	Lecture	application*		
DescribeApplicationOperation	Accorde l'autorisation de décrire le fonctionnement d'une application	Lecture	application*		
DescribeApplicationSnapshot	Accorde l'autorisation de décrire un instantané d'application	Lecture	application*		
DescribeApplicationVersion	Accorde l'autorisation de décrire la version d'une application	Lecture	application*		
DiscoverInputSchema	Accorde l'autorisation de découvrir le schéma d'entrée pour l'application	Lecture			iam:PassRole
ListApplicationOperations	Permet de répertorier les opérations d'une application	Lecture	application*		
ListApplicationSnapshots	Accorde l'autorisation de répertorier les instantanés d'une application	Lecture	application*		
ListApplicationVersions	Accorde l'autorisation de répertorier les versions d'une application	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplications	Accorde l'autorisation de répertorier des demandes pour le compte	Liste			
ListTagsForResource	Accorde l'autorisation de récupérer les balises associées à l'application	Lecture	application*		
RollbackApplication	Accord l'autorisation d'exécuter une opération de restauration sur une application	Écrire	application*		
StartApplication	Accorde l'autorisation de démarrer l'application	Écriture	application*		
StopApplication	Accorde l'autorisation d'arrêter l'application	Écriture	application*		
TagResource	Accorde l'autorisation d'ajouter des balises à l'application	Balisage	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de l'application	Balisage	application*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApplication	Accorde l'autorisation de mettre à jour l'application	Écrire	application*		
UpdateApplicationMaintenanceConfiguration	Accorde l'autorisation de mettre à jour la configuration de maintenance d'une application	Écrire	application*		

Types de ressources définis par Amazon Kinesis Analytics V2

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Kinesis Analytics V2

Amazon Kinesis Analytics V2 définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'un ensemble de valeurs pour chacune des étiquettes	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Kinesis Data Streams

Amazon Kinesis Data Streams (préfixe de service : `kinesis`) fournit les ressources, les actions et les clés de contexte de condition suivantes spécifiques au service à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Kinesis Data Streams
- Types de ressources définis par Amazon Kinesis Data Streams
- Clés de condition pour Amazon Kinesis Data Streams

Actions définies par Amazon Kinesis Data Streams

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTagsToStream	Accorde l'autorisation d'ajouter ou de mettre à jour des balises pour le flux de Amazon Kinesis spécifié. Chaque stream peut contenir jusqu'à 50 tags	Identification	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateStream	Accorde l'autorisation de créer un flux vidéo Amazon Kinesis	Écrire	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DecreaseStreamRetentionPeriod	Accorde l'autorisation de diminuer la période de conservation du flux, qui correspond à la durée pendant	Écrire	stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	laquelle les enregistrements de données sont accessibles après avoir été ajoutés au flux				
DeleteResourcePolicy	Octroie l'autorisation de supprimer une stratégie de ressource associée à un flux ou un consommateur spécifié.	Écrire	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
DeleteStream	Accorde l'autorisation de supprimer un flux et toutes ses partitions et données	Écrire	stream*	aws:ResourceTag/${TagKey}	
DeregisterStreamConsumer	Accorde l'autorisation d'annuler l'enregistrement d'un consommateur de flux avec un flux de données Kinesis	Écrire	consumer*	aws:ResourceTag/${TagKey}	
DescribeAccountSettings	Accorde l'autorisation de décrire les paramètres au niveau du compte pour Amazon Kinesis Data Streams	Lecture			
DescribeLimits	Accorde l'autorisation de décrire les limites et l'utilisation des partitions du compte de l'utilisateur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeStream	Accorde l'autorisation de décrire le flux spécifiée	Lecture	stream*	aws:ResourceTag/${TagKey}	
DescribeStreamConsumer	Accorde l'autorisation d'obtenir la description d'un consommateur de flux enregistré	Lecture	consumer*	aws:ResourceTag/${TagKey}	
DescribeStreamSummary	Accorde l'autorisation de fournir une description résumée du flux de données Kinesis spécifié sans la liste de partition	Lecture	stream*	aws:ResourceTag/${TagKey}	
DisableEnhancedMonitoring	Accorde l'autorisation de désactiver la surveillance améliorée	Écrire			
EnableEnhancedMonitoring	Accorde l'autorisation d'activer la surveillance améliorée du flux de données Kinesis pour les mesures de niveau partagé.	Écrire			
GetRecords	Accorde l'autorisation d'obtenir des enregistrements de données à partir d'une partition	Lecture	stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourcePolicy	Octroie l'autorisation d'obtenir une stratégie de ressource associée à un flux ou un consommateur spécifié.	Lecture	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
GetShardIterator	Accorde l'autorisation d'obtenir un itérateur de partition Celui-ci expire cinq minutes après être retourné au demandeur	Lecture	stream*	aws:ResourceTag/${TagKey}	
IncreaseStreamRetentionPeriod	Accorde l'autorisation d'augmenter la période de conservation du flux, qui correspond à la durée pendant laquelle les enregistrements de données sont accessibles après avoir été ajoutés au flux	Écrire	stream*	aws:ResourceTag/${TagKey}	
InjectApiError [autorisation uniquement]	Accorde l'autorisation d'injecter temporairement des erreurs pour les demandes d'API cibles	Écrire		kinesis:FisActionId kinesis:FisTargetArns kinesis:FisInjectPercentage	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListShards	Accorde l'autorisation de répertorier les partitions d'un flux et fournit des informations sur chaque partition	List	stream*	aws:ResourceTag/${TagKey}	
ListStreamConsumers	Accorde l'autorisation de répertorier les consommateurs de flux enregistrés pour recevoir des données à partir d'un flux Kinesis à l'aide de la diffusion améliorée et fournit des informations sur chaque consommateur	List	stream*	aws:ResourceTag/${TagKey}	
ListStreams	Accorde l'autorisation de répertorier vos flux	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour la ressource Amazon Kinesis spécifiée	Lecture	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
ListTagsForStream	Accorde l'autorisation de répertorier les balises pour le flux de Amazon Kinesis spécifié.	Lecture	stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
MergeShards	Accorde l'autorisation de fusionner deux partitions adjacentes dans un flux et les combine en une seule partition pour réduire la capacité du flux d'ingérer et de transférer des données	Écrire	stream*	aws:ResourceTag/${TagKey}	
PutRecord	Accorde l'autorisation d'écrire un seul enregistrement de données à partir d'un producteur dans un flux Amazon Kinesis	Écrire	stream*	aws:ResourceTag/${TagKey}	
PutRecords	Accorde l'autorisation d'écrire plusieurs enregistrements de données d'un producteur dans un flux Amazon Kinesis en un seul appel (également appelé demande) PutRecords	Écrire	stream*	aws:ResourceTag/${TagKey}	
PutResourcePolicy	Octroie l'autorisation d'associer une stratégie de ressource à un flux ou un consommateur spécifié.	Écrire	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterStreamConsumer	Accorde l'autorisation d'enregistrer un consommateur de flux à l'aide d'un flux de données Kinesis	Écrire	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
RemoveTagsFromStream	Accorde l'autorisation de supprimer des identifications du flux de données Kinesis spécifié Les identifications retirées sont supprimées et ne peuvent pas être récupérées s une fois cette opération terminée	Identification	stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
SplitShard	Accorde l'autorisation de diviser une partition en deux nouvelles partitions dans le flux de données Kinesis, afin d'augmenter la capacité du flux d'ingérer et de transférer des données	Écrire	stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartStreamEncryption	Accorde l'autorisation d'activer ou de mettre à jour le chiffrement côté serveur à l'aide d'une clé AWS KMS pour un flux spécifique	Écrire	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
StopStreamEncryption	Accorde l'autorisation de désactiver le chiffrement côté serveur pour un flux spécifié	Écrire	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
SubscribeToShard	Accorde l'autorisation d'écouter d'une partition spécifique avec la diffusion améliorée	Lecture	consumer*	aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour des balises pour la ressource Amazon Kinesis spécifiée. Chaque ressource peut comporter jusqu'à 50 balises	Identification	consumer*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises de la ressource de données Kinesis spécifiée. Les identifications retirées sont supprimées et ne peuvent pas être récupérées une fois cette opération terminée	Identification	consumer*	aws:TagKeys aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAccountSettings	Autorise la mise à jour des paramètres au niveau du compte pour Amazon Kinesis Data Streams	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMaxRecordSize	Autorise la mise à jour de la taille d'enregistrement maximale pour un flux de données Kinesis	Écrire	stream*	aws:ResourceTag/${TagKey}	
UpdateShardCount	Accorde l'autorisation de mettre à jour le nombre de partitions du flux spécifié avec le nombre spécifié de partitions	Écrire			
UpdateStreamMode	Accorde l'autorisation de mettre à jour le mode de capacité du flux de données	Écrire			
UpdateStreamWarmThroughput	Autorise la mise à jour du débit à chaud d'un flux de données Kinesis à la demande	Écrire	stream*	aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon Kinesis Data Streams

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
stream	`arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}`	aws:ResourceTag/${TagKey}
consumer	`arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}`	aws:ResourceTag/${TagKey}
kmsKey	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	

Clés de condition pour Amazon Kinesis Data Streams

Amazon Kinesis Data Streams définit les clés de condition suivantes qui peuvent être utilisées dans `Condition` l'élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
kinesis:FisActionId	Filtre l'accès en fonction de l'ID d'une AWS action FIS	String

Clés de condition	Description	Type
kinesis:FisInjectPercentage	Filtre l'accès en fonction du pourcentage d'appels concernés par une AWS action FIS	Numérique
kinesis:FisTargetArns	Filtre l'accès par l'ARN d'une AWS cible FIS	ArrayOfARN

Actions, ressources et clés de condition pour Amazon Kinesis Firehose

Amazon Kinesis Firehose (préfixe de service : `firehose`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Kinesis Firehose
- Types de ressources définis par Amazon Kinesis Firehose
- Clés de condition pour Amazon Kinesis Firehose

Actions définies par Amazon Kinesis Firehose

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeliveryStream	Accorde l'autorisation de créer un flux de diffusion	Écrire	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeliveryStream	Accorde l'autorisation de supprimer un flux de diffusion et ses données.	Écriture	deliverystream*		
DescribeDeliveryStream	Accorde l'autorisation de décrire le flux de diffusion spécifié et obtient l'état.	Lecture	deliverystream*		
ListDeliveryStreams	Accorde l'autorisation de répertorier vos flux de diffusion	List			
ListTagsForDeliveryStream	Accorde l'autorisation de répertorier les identifications pour le flux de diffusion spécifié	List	deliverystream*		
PutRecord	Accorde l'autorisation d'écrire un seul enregistrement de données dans un flux de diffusion Amazon Kinesis Firehose	Écrire	deliverystream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutRecordBatch	Accorde l'autorisation d'écrire plusieurs enregistrements de données dans un flux de diffusion au cours d'un appel unique, ce qui peut atteindre un débit supérieur par producteur à celui atteint lors de l'écriture d'enregis trements uniques	Écrire	deliverystream*		
StartDeliveryStreamEncryption	Accorde l'autorisation d'activer le chiffrement côté serveur (SSE) pour le flux de diffusion	Écrire	deliverystream*		
StopDeliveryStreamEncryption	Accorde l'autorisation de désactiver la destination spécifiée du flux de diffusion spécifié	Écrire	deliverystream*		
TagDeliveryStream	Accorde l'autorisation d'ajouter ou de mettre à jour des identifications pour le flux de diffusion spécifié	Identification	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	Accorde l'autorisation de supprimer des identifications du flux de diffusion spécifié	Identification	deliverystream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateDestination	Accorde l'autorisation de mettre à jour la destination spécifiée du flux de diffusion spécifié	Écrire	deliverystream*		

Types de ressources définis par Amazon Kinesis Firehose

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
deliverystream	`arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Kinesis Firehose

Amazon Kinesis Firehose définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Kinesis Video Streams

Amazon Kinesis Video Streams (préfixe de service : `kinesisvideo`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Kinesis Video Streams
- Types de ressources définis par Amazon Kinesis Video Streams
- Clés de condition pour Amazon Kinesis Video Streams

Actions définies par Amazon Kinesis Video Streams

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConnectAsMaster	Accorde l'autorisation de se connecter en tant que maître au canal de signalisation spécifié par le point de terminaison	Écriture	channel*		
ConnectAsViewer	Accorde l'autorisation de se connecter en tant qu'utilisateur au canal de signalisation spécifié par le point de terminaison	Écriture	channel*		
CreateSignalingChannel	Accorde l'autorisation de créer un canal de signalisation	Écriture	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStream	Accorde l'autorisation de créer un flux vidéo Kinesis	Écrire	stream*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DeleteEdgeConfiguration	Accorde l'autorisation de supprimer la configuration de la périphérie de votre flux vidéo Kinesis	Écrire	stream*		
DeleteSignalingChannel	Accorde l'autorisation de supprimer un canal de signalisation existant	Écriture	channel*		
DeleteStream	Accorde l'autorisation de supprimer un flux vidéo Kinesis existant	Écrire	stream*		
DescribeEdgeConfiguration	Accorde l'autorisation de décrire la configuration du périphérique de votre flux vidéo Kinesis	Lecture	stream*		
DescribeImageGenerationConfiguration	Accorde l'autorisation de décrire la configuration de génération d'images de votre flux vidéo Kinesis	Lecture	stream*		
DescribeMappedResourceConfiguration	Accorde l'autorisation de décrire le flux vidéo Kinesis spécifié	List	stream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeMediaStorageConfiguration	Accorde l'autorisation de décrire la configuration de stockage multimédia d'un canal de signalisation	Lecture	channel*		
DescribeNotificationConfiguration	Accorde l'autorisation de décrire la configuration de notification de votre flux vidéo Kinesis	Lecture	stream*		
DescribeSignalingChannel	Accorde l'autorisation de décrire le canal de signalisation spécifié	Liste	channel*		
DescribeStream	Accorde l'autorisation de décrire le flux vidéo Kinesis spécifié	List	stream*		
DescribeStreamStorageConfiguration	Autorise à décrire la configuration du stockage de flux de votre Kinesis Video Stream	Lecture	stream*		
GetClip	Accorde l'autorisation de générer un clip multimédia à partir d'un flux vidéo	Lecture	stream*		
GetDASHStreamingSessionURL	Accorde l'autorisation de créer une URL pour le streaming vidéo MPEG-DASH	Lecture	stream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataEndpoint	Accorde l'autorisation de récupérer un point de terminaison pour un flux spécifié pour lire ou écrire des données multimédia dans Kinesis Video Streams.	Lecture	stream*		
GetHLSStreamingSessionURL	Accorde l'autorisation de créer une URL pour le streaming vidéo HLS	Lecture	stream*		
GetIceServerConfig	Accorde l'autorisation d'obtenir la configuration du serveur ICE	Lecture	channel*		
GetImages	Accorde l'autorisation d'obtenir les images générées à partir de votre flux vidéo Kinesis	Lecture	stream*		
GetMedia	Accorde l'autorisation de renvoyer le contenu multimédia d'un flux vidéo Kinesis	Lecture	stream*		
GetMediaForFragmentList	Accorde l'autorisation de lire et de renvoyer des données multimédia uniquement à partir d'un stockage persistant	Lecture	stream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSignalingChannelEndpoint	Accorde l'autorisation d'obtenir des points de terminaison pour une combinaison spécifiée de protocole et de rôle pour un canal de signalisation	Lecture	channel*		
JoinStorageSession	Accorde l'autorisation de rejoindre une session de stockage pour un canal	Écrire	channel*		
JoinStorageSessionAsViewer	Accorde l'autorisation de rejoindre une session de stockage pour une chaîne en tant que téléspectateur	Écrire	channel*		
ListEdgeAgentConfigurations	Accorde l'autorisation de répertorier les configurations d'un agent de périphérie	List			
ListFragments	Accorde l'autorisation de répertorier les fragments du stockage d'archives en fonction du jeton de pagination ou du type de sélecteur avec la plage spécifiée	Liste	stream*		
ListSignalingChannels	Accorde l'autorisation de répertorier vos canaux de signalisation	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStreams	Accorde l'autorisation de répertorier vos flux vidéo Kinesis	Liste			
ListTagsForResource	Accorde l'autorisation de récupérer les balises associées à votre ressource	Lecture	channel		
			stream		
ListTagsForStream	Accorde l'autorisation de récupérer les balises associées au flux vidéo Kinesis	Lecture	stream*		
PutMedia	Accorde l'autorisation d'envoyer des données multimédia à un flux vidéo Kinesis	Écriture	stream*		
SendAlexaOfferToMaster	Accorde l'autorisation d'envoyer l'offre Alexa SDP au maître	Écrire	channel*		
StartEdgeConfigurationUpdate	Accorde l'autorisation de démarrer la mise à jour de la configuration du périphérique de votre flux vidéo Kinesis	Écrire	stream*		
TagResource	Accorde l'autorisation d'attacher un ensemble de balises à votre ressource	Balisage	channel		
			stream		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
TagStream	Accorde l'autorisation d'attacher un ensemble de balises à vos flux vidéo Kinesis	Balisage	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises de votre ressource	Balisage	channel		
			stream		
				aws:TagKeys	
UntagStream	Accorde l'autorisation de supprimer une ou plusieurs balises de vos flux vidéo Kinesis	Balisage	stream*		
				aws:TagKeys	
UpdateDataRetention	Accorde l'autorisation de mettre à jour la période de conservation des données de votre flux vidéo Kinesis	Écrire	stream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateImageGenerationConfiguration	Accorde l'autorisation de mettre à jour la configuration de génération d'images de votre flux vidéo Kinesis	Écrire	stream*		
UpdateMediaStorageConfiguration	Accorde l'autorisation de créer ou de mettre à jour un mappage entre un canal de signalisation et un flux	Écrire	channel*		
UpdateNotificationConfiguration	Accorde l'autorisation de mettre à jour la configuration de notification de votre flux vidéo Kinesis	Écrire	stream*		
UpdateSignalingChannel	Accorde l'autorisation de mettre à jour un canal de signalisation existant	Écriture	channel*		
UpdateStream	Accorde l'autorisation de mettre à jour un flux vidéo Kinesis existant	Écrire	stream*		
UpdateStreamStorageConfiguration	Autorise la mise à jour de la configuration de stockage des flux de votre Kinesis Video Stream	Écrire	stream*		

Types de ressources définis par Amazon Kinesis Video Streams

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
stream	`arn:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Kinesis Video Streams

Amazon Kinesis Video Streams définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les demandes en fonction de l'ensemble de valeurs autorisées pour chacune des balises.	String
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur-étiquette associée au flux	String
aws:TagKeys	Filtre les demandes en fonction de la présence de clés de balise obligatoires dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS Lake Formation

AWS Lake Formation (préfixe de service :`lakeformation`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Lake Formation
- Types de ressources définis par AWS Lake Formation
- Clés de condition pour AWS Lake Formation

Actions définies par AWS Lake Formation

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddLFTagsToResource	Accorde l'autorisation d'attacher des étiquettes Lake Formation aux ressources du catalogue	Identification			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGrantPermissions	Accorde des autorisations de lac de données à un ou plusieurs mandataires dans un lot	Gestion des autorisations			
BatchRevokePermissions	Accorde l'autorisation de révoquer des autorisations de lac de données à un ou plusieurs mandataires dans un lot	Gestion des autorisations			
CancelTransaction	Accorde l'autorisation d'annuler la transaction donnée	Écrire			
CommitTransaction	Accorde l'autorisation de valider la transaction donnée	Écrire			
CreateDataCellsFilter	Accorde l'autorisation de créer un filtre de cellule de données Lake Formation	Écrire			
CreateLFTag	Accorde l'autorisation de créer une étiquette Lake Formation	Écrire			
CreateLFTagExpression	Autorise la création d'une expression de balise Lake Formation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLakeFormationIdentityCenterConfiguration	Accorde l'autorisation de créer une connexion IAM Identity Center avec Lake Formation pour permettre aux utilisateurs et aux groupes d'IAM Identity Center d'accéder aux ressources du catalogue de données	Écrire			
CreateLakeFormationOptIn	Accorde l'autorisation d'appliquer les autorisations de Lake Formation pour les bases de données, les tables et les principes donnés	Écrire			
DeleteDataCellsFilter	Accorde l'autorisation de supprimer un filtre de cellule de données Lake Formation	Écrire			
DeleteLFTag	Accorde l'autorisation de supprimer une étiquette Lake Formation	Écrire			
DeleteLFTagExpression	Autorise la suppression d'une expression Lake Formation	Écrire			
DeleteLakeFormationIdentityCenterConfiguration	Autorise la suppression d'une connexion IAM Identity Center à Lake Formation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLakeFormationOptIn	Accorde l'autorisation de supprimer l'application des autorisations de Lake Formation aux bases de données, tables et principes donnés	Écrire			
DeleteObjectsOnCancel	Accorde l'autorisation de supprimer les objets spécifiés si la transaction est annulée	Écrire			
DeregisterResource	Accorde l'autorisation de désenregistrer un emplacement enregistré	Écrire			
DescribeLakeFormationIdentityCenterConfiguration	Accorde l'autorisation de décrire la connexion entre l'IAM Identity Center et Lake Formation	Lecture			
DescribeResource	Accorde l'autorisation de décrire un emplacement enregistré	Lecture			
DescribeTransaction	Accorde l'autorisation d'obtenir le statut de la transaction donnée	Lecture			
ExtendTransaction	Accorde l'autorisation de prolonger le délai d'expiration de la transaction donnée	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataAccess	Accorde l'autorisation d'accéder au lac de données virtuel	Écrire		lakeformation:EnabledOnlyForMetaDataAccess	
GetDataCellsFilter	Octroie l'autorisation de récupérer un filtre de cellule de données Lake Formation	Lecture			
GetDataLakePrincipal	Accorde l'autorisation de récupérer l'identité du principal invocateur	Lecture			
GetDataLakeSettings	Accorde l'autorisation de récupérer les paramètres de lac de données tels que la liste des administrateurs de lac de données et les autorisations par défaut de base de données et de table	Lecture			
GetEffectivePermissionsForPath	Accorde l'autorisation de récupérer les autorisations attachées aux ressources dans le chemin d'accès donné	Lecture			
GetLFTag	Accorde l'autorisation de récupérer une étiquette Lake Formation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLFTagExpression	Autorise la récupération d'une expression de balise Lake Formation	Lecture			
GetQueryState	Accorde l'autorisation de récupérer l'état de la requête donnée	Lecture			lakeformation:StartQueryPlanning
GetQueryStatistics	Accorde l'autorisation de récupérer les statistiques de la requête donnée	Lecture			lakeformation:StartQueryPlanning
GetResourceLFTags	Accorde l'autorisation de récupérer les balises lakeformation sur une ressource de catalogue	Lecture			
GetTableObjects	Accorde l'autorisation de récupérer des objets à partir d'une table	Lecture			
GetTemporaryGluePartitionCredentials	Permet d'obtenir des informations d'identification temporaires pour accéder aux données de la partition Glue via Lake Formation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTemporaryGlueTableCredentials	Permet d'obtenir des informations d'identification temporaires pour accéder aux données de la table Glue via Lake Formation	Lecture			
GetWorkUnitResults	Accorde l'autorisation de récupérer les résultats des unités de travail données	Lecture			lakeformation:GetWorkUnits lakeformation:StartQueryPlanning
GetWorkUnits	Accorde l'autorisation de récupérer les unités de travail de la requête donnée	Lecture			lakeformation:StartQueryPlanning
GrantPermissions	Accorde l'accès à des autorisations de lac de données à un principal	Gestion des autorisations			
ListDataCellsFilter	Accorde l'autorisation de répertorier des filtres de cellules	List			
ListLFTagExpressions	Accorde l'autorisation de répertorier les expressions de balises Lake Formation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLFTags	Accorde l'autorisation de répertorier les étiquettes Lake Formation	Lecture			
ListLakeFormationOptIns	Accorde l'autorisation de récupérer la liste actuelle des ressources et des principaux autorisés à appliquer les autorisations de Lake Formation	List			
ListPermissions	Accorde l'autorisation de répertorier les autorisations filtrées par principal ou ressource	List			
ListResources	Accorde l'autorisation de répertorier les emplacements enregistrés	List			
ListTableStorageOptimizers	Accorde l'autorisation de répertorier tous les optimiseurs de stockage de la table régie	List			
ListTransactions	Accorde l'autorisation de répertorier toutes les transactions du système	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDataLakeSettings	Accorde l'autorisation de remplacer les paramètres de lac de données tels que la liste des administrateurs de lac de données et les autorisations par défaut de base de données et de table	Gestion des autorisations			
RegisterResource	Accorde l'autorisation d'enregistrer un nouvel emplacement à gérer par Lake Formation	Écrire			
RegisterResourceWithPrivilegedAccess	Autorise l'enregistrement d'un nouvel emplacement qui sera géré par Lake Formation, avec un accès privilégié	Écrire			
RemoveLFTagsFromResource	Accorde l'autorisation de supprimer les balises lakeformation des ressources du catalogue	Identification			
RevokePermissions	Accorde l'autorisation de révoquer des autorisations de lac de données à un principal	Gestion des autorisations			
SearchDatabasesByLFTags	Accorde l'autorisation de répertorier les bases de données de catalogue avec des étiquettes Lake Formation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchTablesByLFTags	Accorde l'autorisation de répertorier les tables de catalogue avec des étiquettes Lake Formation	Lecture			
StartQueryPlanning	Accorde l'autorisation de lancer la planification de la requête donnée	Écrire			
StartTransaction	Accorde l'autorisation de démarrer une nouvelle transaction	Écrire			
UpdateDataCellsFilter	Octroie l'autorisation de mettre à jour un filtre de cellule de données Lake Formation	Écrire			
UpdateLFTag	Accorde l'autorisation de mettre à jour une étiquette Lake Formation	Écrire			
UpdateLFTagExpression	Autorise la mise à jour d'une expression de Lake Formation	Écrire			
UpdateLakeFormationIdentityCenterConfiguration	Accorde l'autorisation de mettre à jour les paramètres de connexion IAM Identity Center	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateResource	Accorde l'autorisation de mettre à jour un emplacement enregistré	Écrire			
UpdateTableObjects	Accorde l'autorisation d'ajouter ou de supprimer les objets spécifiés vers ou depuis une table	Écrire			
UpdateTableStorageOptimizer	Accorde l'autorisation de mettre à jour la configuration de l'optimiseur de stockage de la table régie	Écrire			

Types de ressources définis par AWS Lake Formation

AWS Lake Formation ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Lake Formation, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Lake Formation

AWS Lake Formation définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
lakeformation:EnabledOnlyForMetaDataAccess	Filtre l'accès en fonction de la présence de la clé configurée pour la politique basée sur l'identité du rôle	Booléen

Actions, ressources et clés de condition pour AWS Lambda

AWS Lambda (préfixe de service :`lambda`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Lambda
- Types de ressources définis par AWS Lambda
- Clés de condition pour AWS Lambda

Actions définies par AWS Lambda

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddLayerVersionPermission	Accorde l'autorisation d'ajouter des autorisations à la politique basée sur les ressources d'une version d'une couche Lambda AWS	Gestion des autorisations	layerVersion*		
AddPermission	Accorde l'autorisation d'autoriser un AWS service ou un autre compte à utiliser une fonction AWS Lambda	Gestion des autorisations	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
CheckpointDurableExecution	Accorde l'autorisation d'enregistrer la progression d'une exécution durable de AWS Lambda	Écrire	durable execution*		
CreateAlias	Accorde l'autorisation de créer un alias pour une version de fonction Lambda	Écrire	function*		
CreateCapacityProvider	Accorde l'autorisation de créer un fournisseur de AWS capacité Lambda	Écrire	capacityProvider*		iam:CreateServiceLinkedRole iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys lambda:SecurityGroupIds lambda:SubnetIds	
CreateCodeSigningConfig	Accorde l'autorisation de créer une configuration de signature de code AWS Lambda	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventSourceMapping	Accorde l'autorisation de créer un mappage entre une source d'événement et une fonction AWS Lambda	Écrire		lambda:FunctionArn aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFunction	Accorde l'autorisation de créer une fonction AWS Lambda	Écrire	function*		iam:PassRole lambda:PassCapacityProvider
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFunctionUrlConfig	Accorde l'autorisation de créer une configuration d'URL de fonction pour une fonction Lambda	Écrire	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteAlias	Autorise la suppression d'un alias de AWS fonction Lambda	Écrire	function*		
DeleteCapacityProvider	Accorde l'autorisation de supprimer un fournisseur de AWS capacité Lambda	Écrire	capacityProvider*		
DeleteCodeSigningConfig	Accorde l'autorisation de supprimer une configuration de signature de code AWS Lambda	Écrire	code signing config*		
DeleteEventSourceMapping	Accorde l'autorisation de supprimer un mappage de source d'événement AWS Lambda	Écrire	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	Accorde l'autorisation de supprimer une fonction AWS Lambda	Écrire	function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFunctionCodeSigningConfig	Accorde l'autorisation de détacher une configuration de signature de code d'une fonction AWS Lambda	Écrire	function*		
DeleteFunctionConcurrency	Accorde l'autorisation de supprimer une limite d'exécution simultanée d'une fonction AWS Lambda	Écrire	function*		
DeleteFunctionEventInvokeConfig	Accorde l'autorisation de supprimer la configuration pour un appel asynchrone pour une fonction, une version ou un AWS alias Lambda	Écrire	function*		
DeleteFunctionUrlConfig	Accorde l'autorisation de supprimer une configuration d'URL de fonction pour une fonction Lambda	Écrire	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteLayerVersion	Accorde l'autorisation de supprimer une version d'une couche AWS Lambda	Écrire	layerVersion*		
DeleteProvisionedConcurrencyConfig	Accorde l'autorisation de supprimer la configuration de simultanéité provisionnée pour une fonction Lambda AWS	Écrire	function alias		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			function version		
DisableReplication [autorisation uniquement]	Accorde l'autorisation de désactiver la réplication pour une fonction Lambda@Edge	Gestion des autorisations	function*		
EnableReplication [autorisation uniquement]	Accorde l'autorisation d'activer la réplication pour une fonction Lambda@Edge	Gestion des autorisations	function*		
GetAccountSettings	Accorde l'autorisation de consulter les détails relatifs aux limites et à l'utilisation d'un compte dans un Région AWS	Lecture			
GetAlias	Autorise l'affichage des détails relatifs à un alias de AWS fonction Lambda	Lecture	function*		
GetCapacityProvider	Autorise l'accès aux informations relatives à un fournisseur de AWS capacité Lambda	Lecture	capacityProvider*		
GetCodeSigningConfig	Accorde l'autorisation d'afficher les détails d'une configuration de signature de code AWS Lambda	Lecture	code signing config*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDurableExecution	Accorde l'autorisation d'afficher les détails d'une exécution AWS durable Lambda	Lecture	durable execution*		
GetDurableExecutionHistory	Autorise l'affichage de l'historique d'exécution d'une exécution AWS durable Lambda	Lecture	durable execution*		
GetDurableExecutionState	Autorise l'affichage de l'état actuel d'une exécution AWS durable Lambda	Lecture	durable execution*		
GetEventSourceMapping	Accorde l'autorisation d'afficher les détails relatifs au mappage d'une AWS source d'événements Lambda	Lecture	eventSourceMapping*		
				lambda:FunctionArn	
GetFunction	Accorde l'autorisation d'afficher les détails d'une fonction AWS Lambda	Lecture	function*		
GetFunctionCodeSigningConfig	Autorise l'affichage de la configuration de signature de code (arn) attachée à une fonction AWS Lambda	Lecture	function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFunctionConcurrency	Accorde l'autorisation d'afficher des détails sur la configuration de la simultanéité réservée pour une fonction	Lecture	function*		
GetFunctionConfiguration	Accorde l'autorisation d'afficher les détails des paramètres spécifiques à la version d'une fonction ou d'une version AWS Lambda	Lecture	function*		
GetFunctionEventInvokeConfig	Accorde l'autorisation d'afficher la configuration d'une invocation asynchrone pour une fonction, une version ou un alias	Lecture	function*		
GetFunctionRecursionConfig	Autorise l'affichage de la configuration de récursivité d'une fonction AWS Lambda	Lecture	function*		
GetFunctionScalingConfig	Autorise l'affichage de la configuration de dimensionnement d'une fonction AWS Lambda exécutée sur un fournisseur de capacité	Lecture	function*		
GetFunctionUrlConfig	Accorde l'autorisation de lire une configuration d'URL de fonction pour une fonction Lambda	Lecture	function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				lambda:FunctionUrlAuthType lambda:FunctionArn	
GetLayerVersion	Accorde l'autorisation d'afficher les détails d'une version d'une couche AWS Lambda. Notez que cette action prend également en charge GetLayerVersionByArn l'API	Lecture	layerVersion*		
GetLayerVersionPolicy	Accorde l'autorisation de consulter la politique basée sur les ressources pour une version d'une couche Lambda AWS	Lecture	layerVersion*		
GetPolicy	Accorde l'autorisation de consulter la politique basée sur les ressources pour une fonction, une version ou un AWS alias Lambda	Lecture	function*		
GetProvisionedConcurrencyConfig	Accorde l'autorisation de consulter la configuration de simultanéité provisionnée pour l'alias ou la version d'une fonction AWS Lambda	Lecture	function alias		
			function version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRuntimeManagementConfig	Accorde l'autorisation de consulter la configuration de gestion de l'exécution d'une fonction AWS Lambda	Lecture	function*		
InvokeAsync	Accorde l'autorisation d'invoquer une fonction de manière asynchrone (Obsolète)	Écrire	function*		
InvokeFunction	Accorde l'autorisation d'invoquer une fonction AWS Lambda	Écrire	function*		
				lambda:EventSourceToken lambda:InvokedViaFunctionUrl	
InvokeFunctionUrl [autorisation uniquement]	Accorde l'autorisation d'invoquer une fonction AWS Lambda via une URL	Écrire	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAliases	Accorde l'autorisation de récupérer une liste d'alias pour une fonction AWS Lambda	List	function*		
ListCapacityProviders	Accorde l'autorisation de récupérer une liste de fournisseurs de AWS capacité Lambda	List			
ListCodeSigningConfigs	Accorde l'autorisation de récupérer une liste de configurations de AWS signature de code Lambda	List			
ListDurableExecutionsByFunction	Accorde l'autorisation de récupérer une liste d'exécutions durables AWS Lambda d'une fonction AWS Lambda	List	function*		
ListEventSourceMappings	Accorde l'autorisation de récupérer une liste de mappages de AWS sources d'événements Lambda	List			
ListFunctionEventInvokeConfigs	Accorde l'autorisation de récupérer une liste de configurations pour l'invocation asynchrone d'une fonction	List	function*		
ListFunctionUrlConfigs	Accorde l'autorisation de lire les configurations d'URL d'une fonction pour une fonction	List	function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				lambda:FunctionUrlAuthType	
ListFunctionVersionsByCapacityProvider	Accorde l'autorisation de récupérer une liste des versions de fonctions AWS Lambda par le fournisseur de capacité attribué	List	capacityProvider*		
ListFunctions	Accorde l'autorisation de récupérer une liste de fonctions AWS Lambda, avec la configuration spécifique à la version de chaque fonction	List			
ListFunctionsByCodeSigningConfig	Accorde l'autorisation de récupérer une liste de fonctions AWS Lambda en fonction de la configuration de signature de code assignée	List	codesigningconfig*		
ListLayerVersions	Accorde l'autorisation de récupérer la liste des versions d'une couche AWS Lambda	List			
ListLayers	Accorde l'autorisation de récupérer une liste de couches AWS Lambda, avec des détails sur la dernière version de chaque couche	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProvisionedConcurrencyConfigs	Accorde l'autorisation de récupérer une liste de configurations de simultanéité provisionnées pour une fonction Lambda AWS	List	function*		
ListTags	Accorde l'autorisation de récupérer une liste de balises pour une fonction AWS Lambda, un mappage de source d'événements, un fournisseur de capacité ou une ressource de configuration de signature de code	Lecture	capacityProvider		
			codesigningconfig		
			eventSourceMapping		
			function		
ListVersionsByFunction	Accorde l'autorisation de récupérer une liste de versions pour une fonction AWS Lambda	List	function*		
PassCapacityProvider [autorisation uniquement]	Accorde l'autorisation de transférer un fournisseur de capacité AWS Lambda à un service	Écrire	capacityProvider*		
PublishLayerVersion	Accorde l'autorisation de créer une couche AWS Lambda	Écrire	layer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PublishVersion	Accorde l'autorisation de créer une version de AWS fonction Lambda	Écrire	function*		
PutFunctionCodeSigningConfig	Accorde l'autorisation d'associer une configuration de signature de code à une fonction AWS Lambda	Écrire	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	Accorde l'autorisation de configurer la simultanéité réservée pour une fonction AWS Lambda	Écrire	function*		
PutFunctionEventInvokeConfig	Accorde l'autorisation de configurer les options d'appel asynchrone sur une fonction, une version ou un alias AWS Lambda	Écrire	function*		
PutFunctionRecursionConfig	Accorde l'autorisation de mettre à jour la configuration de récursivité d'une fonction AWS Lambda	Écrire	function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutFunctionScalingConfig	Accorde l'autorisation de mettre à jour la configuration de dimensionnement d'une fonction AWS Lambda exécutée sur un fournisseur de capacité	Écrire	function*		
PutProvisionedConcurrencyConfig	Accorde l'autorisation de configurer la simultanéité provisionnée pour l'alias ou la version d'une fonction AWS Lambda	Écrire	function alias		
			function version		
PutRuntimeManagementConfig	Accorde l'autorisation de mettre à jour la configuration de gestion d'exécution d'une fonction AWS Lambda	Écrire	function*		
RemoveLayerVersionPermission	Accorde l'autorisation de supprimer une instruction de la politique d'autorisations pour une version d'une couche AWS Lambda	Gestion des autorisations	layerVersion*		
RemovePermission	Accorde l'autorisation de révoquer l'autorisation d'utilisation des fonctions d'un AWS service ou d'un autre compte	Gestion des autorisations	function*		
				lambda:Principal lambda:FunctionUrlAuthType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendDurableExecutionCallbackFailure	Accorde l'autorisation d'envoyer une réponse d'échec pour une opération de rappel dans une exécution durable AWS Lambda	Écrire	durable execution*		
SendDurableExecutionCallbackHeartbeat	Accorde l'autorisation d'envoyer un battement de cœur pour une opération de rappel dans une exécution durable Lambda AWS	Écrire	durable execution*		
SendDurableExecutionCallbackSuccess	Accorde l'autorisation d'envoyer une réponse réussie pour une opération de rappel dans une exécution durable AWS Lambda	Écrire	durable execution*		
StopDurableExecution	Accorde l'autorisation d'arrêter une exécution AWS durable de Lambda	Écrire	durable execution*		
TagResource	Accorde l'autorisation d'ajouter des balises à une fonction AWS Lambda, à un mappage de sources d'événements, à un fournisseur de capacité ou à une ressource de configuration de signature de code	Identification	capacityProvider		
			code signing config		
			eventSourceMapping		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			function		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises d'une fonction AWS Lambda, d'un mappage de sources d'événements, d'un fournisseur de capacité ou d'une ressource de configuration de signature de code	Identification	capacityProvider		
			codesigningconfig		
			eventSourceMapping		
			function		
				aws:TagKeys	
UpdateAlias	Accorde l'autorisation de mettre à jour la configuration de l'alias d'une fonction AWS Lambda	Écrire	function*		
UpdateCapacityProvider	Autorise la mise à jour d'un fournisseur de AWS capacité Lambda	Écrire	capacityProvider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCodeSigningConfig	Autorise la mise à jour d'une configuration de signature de code AWS Lambda	Écrire	code signing config*		
UpdateEventSourceMapping	Accorde l'autorisation de mettre à jour la configuration d'un mappage de source d'événements AWS Lambda	Écrire	eventSourceMapping*		
				lambda:FunctionArn	
UpdateFunctionCode	Accorde l'autorisation de mettre à jour le code d'une fonction AWS Lambda	Écrire	function*		
UpdateFunctionCodeSigningConfig	Accorde l'autorisation de mettre à jour la configuration de signature de code d'une fonction AWS Lambda	Écrire	code signing config*		
			function*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFunctionConfiguration	Accorde l'autorisation de modifier les paramètres spécifiques à la version d'une fonction Lambda AWS	Écrire	function*		
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	
UpdateFunctionEventInvokeConfig	Accorde l'autorisation de modifier la configuration pour l'appel asynchrone pour une fonction, une version ou un AWS alias Lambda	Écrire	function*		
UpdateFunctionUrlConfig	Accorde l'autorisation de mettre à jour une configuration d'URL de fonction pour une fonction Lambda	Écrire	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Types de ressources définis par AWS Lambda

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
capacityProvider	`arn:${Partition}:lambda:${Region}:${Account}:capacity-provider:${CapacityProviderName}`	aws:ResourceTag/${TagKey}
code signing config	`arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}`	aws:ResourceTag/${TagKey}
durable execution	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}/durable-execution/${ExecutionName}/${ExecutionId}`	
eventSourceMapping	`arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}`	aws:ResourceTag/${TagKey}
function	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}`	aws:ResourceTag/${TagKey}
function alias	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
function version	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}`	aws:ResourceTag/${TagKey}
layer	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}`	
layerVersion	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}`	

Clés de condition pour AWS Lambda

AWS Lambda définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Clés de condition	Description	Type
lambda:CodeSigningConfigArn	Filtre l'accès par l'ARN d'une configuration de signature de code AWS Lambda	ARN
lambda:EventSourceToken	Filtre l'accès par ID à partir d'une source non AWS événementielle configurée pour la fonction AWS Lambda	String
lambda:FunctionArn	Filtre l'accès par l'ARN d'une fonction AWS Lambda	ARN
lambda:FunctionUrlAuthType	Filtre l'accès par type d'autorisation spécifié dans la demande. Disponible pendant CreateFunctionUrlConfig, UpdateFunctionUrlConfig DeleteFunctionUrlConfig, GetFunctionUrlConfig ListFunctionUrlConfig, AddPermission et les RemovePermission opérations	String
lambda:InvokedViaFunctionUrl	Limite le champ d'application de lambda : InvokeFunction action à Function URLs uniquement. Disponible pendant le AddPermission fonctionnement	Booléen
lambda:Layer	Filtre l'accès par l'ARN d'une version d'une couche AWS Lambda	ArrayOfString
lambda:Principal	Filtre l'accès en restreignant le AWS service ou le compte qui peut invoquer une fonction	String
lambda:SecurityGroupIds	Filtre l'accès en fonction de l'ID des groupes de sécurité configurés pour la fonction AWS Lambda	ArrayOfString
lambda:SourceFunctionArn	Filtre l'accès par l'ARN de la fonction AWS Lambda d'où provient la demande	ARN
lambda:SubnetIds	Filtre l'accès en fonction de l'ID des sous-réseaux configurés pour la fonction AWS Lambda	ArrayOfString
lambda:VpcIds	Filtre l'accès en fonction de l'ID du VPC configuré pour la fonction Lambda AWS	String

Actions, ressources et clés de condition pour AWS Launch Wizard

AWS Launch Wizard (préfixe de service :`launchwizard`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Launch Wizard
- Types de ressources définis par AWS Launch Wizard
- Clés de condition pour AWS Launch Wizard

Actions définies par AWS Launch Wizard

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAdditionalNode [autorisation uniquement]	Accorde l'autorisation de créer un nœud supplémentaire	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeployment	Accorde l'autorisation de créer un déploiement	Écrire	deployment*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSettingsSet [autorisation uniquement]	Accorde l'autorisation de créer un ensemble de paramètres d'application	Écrire			
DeleteAdditionalNode [autorisation uniquement]	Accorde l'autorisation de supprimer un nœud supplémentaire	Écrire			
DeleteApp [autorisation uniquement]	Accorde l'autorisation de supprimer une application	Écrire			
DeleteDeployment	Octroie l'autorisation de supprimer un déploiement.	Écrire	deployment*	aws:ResourceTag/${TagKey}	
DeleteSettingsSet [autorisation uniquement]	Accorde l'autorisation de supprimer un ensemble de paramètres	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAdditionalNode [autorisation uniquement]	Accorde l'autorisation de décrire un nœud supplémentaire	Lecture			
DescribeProvisionedApp [autorisation uniquement]	Accorde l'autorisation de décrire des applications de provisionnement	Lecture			
DescribeProvisioningEvents [autorisation uniquement]	Accorde l'autorisation de décrire des évènements de provisionnement	Lecture			
DescribeSettingsSet [autorisation uniquement]	Accorde l'autorisation de décrire un ensemble de paramètres d'application	Lecture			
GetDeployment	Accorde l'autorisation d'obtenir un déploiement	Lecture	deployment*	aws:ResourceTag/${TagKey}	
GetDeploymentPatternVersion	Accorde l'autorisation d'obtenir une version d'un modèle de déploiement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInfrastructureSuggestion [autorisation uniquement]	Accorde l'autorisation d'obtenir une suggestion d'infrastructure	Lecture			
GetIpAddress [autorisation uniquement]	Accorde l'autorisation d'obtenir l'adresse IP du client	Lecture			
GetResourceCostEstimate [autorisation uniquement]	Accorde l'autorisation d'obtenir une estimation de coûts des ressources	Lecture			
GetResourceRecommendation [autorisation uniquement]	Accorde l'autorisation d'obtenir une recommandation pour une ressource	Lecture			
GetSettingsSet [autorisation uniquement]	Accorde l'autorisation d'obtenir un ensemble de paramètres	Lecture			
GetWorkload	Accorde l'autorisation pour obtenir une charge de travail	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkloadAsset [autorisation uniquement]	Accorde l'autorisation d'obtenir une ressource de charge de travail	Lecture			
GetWorkloadAssets [autorisation uniquement]	Accorde l'autorisation d'obtenir des ressources de charge de travail	Lecture			
GetWorkloadDeploymentPattern	Accorde l'autorisation d'obtenir un modèle de déploiement	Lecture			
ListAdditionalNodes [autorisation uniquement]	Accorde l'autorisation de répertorier les nœuds supplémentaires	List			
ListAllowedResources [autorisation uniquement]	Accorde l'autorisation de répertorier les ressources autorisées	List			
ListDeploymentEvents	Accorde l'autorisation de répertorier les évènements survenus durant un déploiement	List			
ListDeploymentPatternVersions	Accorde l'autorisation de répertorier les versions d'un modèle de déploiement	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDeployments	Accorde l'autorisation de répertorier les déploiements	List			
ListProvisionedApps [autorisation uniquement]	Accorde l'autorisation de répertorier les applications de provisionnement	List			
ListResourceCostEstimates [autorisation uniquement]	Accorde l'autorisation de répertorier les estimations de coûts des ressources	List			
ListSettingsSets [autorisation uniquement]	Accorde l'autorisation de répertorier les ensembles de paramètres	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une LaunchWizard ressource	Lecture	deployment	aws:ResourceTag/${TagKey}	
ListWorkloadDeploymentOptions [autorisation uniquement]	Accorde l'autorisation de répertorier les options de déploiement d'une charge de travail donnée	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWorkloadDeploymentPatterns	Accorde l'autorisation de répertorier les modèles de déploiement d'une charge de travail	List			
ListWorkloads	Accorde l'autorisation de répertorier les charges de travail	List			
PutSettingsSet [autorisation uniquement]	Accorde l'autorisation de créer un ensemble de paramètres	Écrire			
StartProvisioning [autorisation uniquement]	Accorde l'autorisation de lancer un provisionnement	Écrire			
TagResource	Accorde l'autorisation de baliser une LaunchWizard ressource	Identification	deployment	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource LaunchWizard	Identification	deployment	aws:TagKeys	
UpdateDeployment	Accorde l'autorisation de mettre à jour un déploiement	Écrire	deployment*	aws:ResourceTag/${TagKey}	
UpdateSettingsSet [autorisation uniquement]	Accorde l'autorisation de mettre à jour un ensemble de paramètres d'application	Écrire			

Types de ressources définis par AWS Launch Wizard

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
deployment	`arn:${Partition}:launchwizard:${Region}:${Account}:deployment/${DeploymentId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Launch Wizard

AWS Launch Wizard définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Lex

Amazon Lex (préfixe de service : `lex`) fournit les ressources, actions et clés de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Lex
- Types de ressources définis par Amazon Lex
- Clés de condition pour Amazon Lex

Actions définies par Amazon Lex

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBotVersion	Crée une version basée sur la version $LATEST du robot spécifié	Écrire	bot version*		
CreateIntentVersion	Crée une version basée sur la version $LATEST de l'intention spécifiée	Écrire	intent version*		
CreateSlotTypeVersion	Crée une version basée sur la version $LATEST du type d'emplacement spécifié	Écrire	slottype version*		
DeleteBot	Supprime toutes les versions d'un robot	Écrire	bot version*		
DeleteBotAlias	Supprime un alias pour un robot spécifique	Écrire	bot alias*		
DeleteBotChannelAssociation	Supprime l'association entre un alias de robot Amazon Lex et une plateforme de messagerie	Écrire	channel*		
DeleteBotVersion	Supprime une version spécifique d'un robot	Écrire	bot version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteIntent	Supprime toutes les versions d'une intention	Écrire	intent version*		
DeleteIntentVersion	Supprime une version spécifique d'une intention	Écrire	intent version*		
DeleteSession	Supprime les informations de session pour un bot, un alias et un ID utilisateur spécifiés	Écrire	bot alias		
			bot version		
DeleteSlotType	Supprime toutes les versions d'un type d'emplacement	Écrire	slottype version*		
DeleteSlotTypeVersion	Supprime une version spécifique d'un type d'emplacement	Écrire	slottype version*		
DeleteUtterances	Supprime les informations qu'Amazon Lex tient à jour pour des énoncés sur un robot et pour un userId spécifiques	Écrire	bot version*		
GetBot	Renvoie des informations pour un robot spécifique. En plus du nom du robot, l'alias ou la version du robot est nécessaire	Lecture	bot alias		
			bot version		
GetBotAlias	Renvoie des informations sur un alias de robot Amazon Lex	Lecture	bot alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBotAliases	Renvoie la liste des alias pour un robot Amazon Lex donné	List			
GetBotChannelAssociation	Renvoie des informations sur l'association entre un robot Amazon Lex et une plateforme de messagerie	Lecture	channel*		
GetBotChannelAssociations	Renvoie la liste de tous les canaux associés à un robot individuel	List	channel*		
GetBotVersions	Renvoie des informations pour toutes les versions d'un robot spécifique	List	bot version*		
GetBots	Renvoie des informations pour la version $LATEST de tous les robots soumis à des filtres fournis par le client	List			
GetBuiltInIntent	Renvoie des informations sur une intention intégrée	Lecture			
GetBuiltInIntents	Obtient la liste des intentions intégrées qui répondent aux critères spécifiés	Lecture			
GetBuiltInSlotTypes	Obtient la liste des types d'emplacement intégrés qui répondent aux critères spécifiés	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExport	Exporte la ressource Amazon Lex dans un format demandé	Lecture	bot version*		
GetImport	Obtient des informations sur une tâche d'importation démarrée avec StartImport	Lecture			
GetIntent	Renvoie des informations pour une intention spécifique. En plus du nom de l'intention, vous devez également spécifier la version de l'intention	Lecture	intent version*		
GetIntentVersions	Renvoie des informations pour toutes les versions d'une intention spécifique	List	intent version*		
GetIntents	Renvoie des informations pour la version $LATEST de toutes les intentions soumises à des filtres fournis par le client	List			
GetMigration	Accorde l'autorisation d'afficher une migration en cours ou terminée	Lecture			
GetMigrations	Accorde l'autorisation d'afficher la liste des migrations depuis Amazon Lex v1 vers Amazon Lex v2	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSession	Renvoie les informations de session pour un robot, un alias et un ID utilisateur spécifiés	Lecture	bot alias		
			bot version		
GetSlotType	Renvoie des informations sur une version spécifique d'un type d'emplacement. En plus de spécifier le nom du type d'emplacement, vous devez également spécifier la version du type d'emplacement	Lecture	slottype version*		
GetSlotTypeVersions	Renvoie des informations pour toutes les versions d'un type d'emplacement spécifique	List	slottype version*		
GetSlotTypes	Renvoie des informations pour la version $LATEST de tous les types d'emplacement soumis à des filtres fournis par le client	List			
GetUtterancesView	Renvoie une vue de données d'énoncé d'agrégation pour les versions d'un robot pour une période récente	List	bot version*		
ListTagsForResource	Répertorie les balises d'une ressource Lex	Lecture	bot		
			bot alias		
			channel		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PostContent	Envoie l'entrée utilisateur (texte ou voix) à Amazon Lex	Écrire	bot alias		
			bot version		
PostText	Envoie l'entrée utilisateur (texte uniquement) à Amazon Lex	Écrire	bot alias		
			bot version		
PutBot	Crée ou met à jour la version $LATEST d'un robot conversationnel Amazon Lex	Écrire	bot version*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutBotAlias	Crée ou met à jour un alias pour le robot spécifique	Écrire	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutIntent	Crée ou met à jour la version $LATEST d'une intention	Écrire	intent version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutSession	Crée une nouvelle session ou modifie une session existante avec un robot Amazon Lex	Écrire	bot alias		
			bot version		
PutSlotType	Crée ou met à jour la version $LATEST d'un type d'emplacement	Écrire	slottype version*		
StartImport	Démarre une tâche pour importer une ressource dans Amazon Lex	Écrire			
StartMigration	Accorde l'autorisation de migrer un robot depuis Amazon Lex v1 vers Amazon Lex v2	Écrire	bot version*		
TagResource	Ajoute ou remplace des balises pour une ressource Lex	Balisage	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Supprime des balises d'une ressource Lex	Balisage	bot		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	

Types de ressources définis par Amazon Lex

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
bot	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}`	aws:ResourceTag/${TagKey}
bot version	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotVersion}`	aws:ResourceTag/${TagKey}
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotAlias}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
channel	arn:${Partition}:lex:${Region}:${Account}:bot-channel:${BotName}:${BotAlias}:${ChannelName}	aws:ResourceTag/${TagKey}
intent version	arn:${Partition}:lex:${Region}:${Account}:intent:${IntentName}:${IntentVersion}	
slottype version	arn:${Partition}:lex:${Region}:${Account}:slottype:${SlotName}:${SlotVersion}	

Clés de condition pour Amazon Lex

Amazon Lex définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises de la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource Lex	String
aws:TagKeys	Filtre l'accès en fonction de l'ensemble des clés d'identification dans la demande	ArrayOfString

Clés de condition	Description	Type
lex:associatedIntents	Vous permet de contrôler l'accès en fonction des intentions incluses dans la demande	ArrayOfString
lex:associatedSlotTypes	Vous permet de contrôler l'accès en fonction des types d'emplacement inclus dans la demande	ArrayOfString
lex:channelType	Vous permet de contrôler l'accès en fonction du type de canal inclus dans la demande	String

Actions, ressources et clés de condition pour Amazon Lex V2

Amazon Lex V2 (préfixe de service : `lex`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Lex V2
- Types de ressources définis par Amazon Lex V2
- Clés de condition pour Amazon Lex V2

Actions définies par Amazon Lex V2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchCreateCustomVocabularyItem	Accorde l'autorisation de créer de nouveaux éléments dans un vocabulaire personnalisé existant	Écrire	bot*		
BatchDeleteCustomVocabularyItem	Accorde l'autorisation de supprimer des éléments existants dans un vocabulaire personnalisé existant	Écrire	bot*		
BatchUpdateCustomVocabularyItem	Accorde l'autorisation de mettre à jour des éléments existants dans un vocabulaire personnalisé existant	Écrire	bot*		
BuildBotLocale	Accorde l'autorisation de construire une locale de robot existante dans un robot	Écriture	bot*		
CreateBot	Accorde l'autorisation de créer un nouveau robot et un alias de robot test indiquant la version du robot DRAFT	Écriture	bot* bot alias*	 aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotAlias	Accorde l'autorisation de créer un nouvel alias de robot dans un robot	Écriture	bot alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotChannel [autorisation uniquement]	Accorde l'autorisation de créer un canal de robot dans un robot existant	Écriture	bot*		
CreateBotLocale	Accorde l'autorisation de créer une nouvelle locale de robot dans un robot existant	Écrire	bot*		
CreateBotReplica	Accorde l'autorisation de créer une réplique de bot pour un bot	Écrire	bot*		
CreateBotVersion	Accorde l'autorisation de créer une nouvelle version d'un robot existant	Écrire	bot*		
CreateCustomVocabulary [autorisation uniquement]	Accorde l'autorisation de créer un vocabulaire personnalisé dans une locale de robot existante	Écrire	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateExport	Accorde l'autorisation de créer une exportation pour une ressource existante	Écriture	bot		
			test set		
CreateIntent	Accorde l'autorisation de créer une nouvelle intention dans une locale de robot existante	Écriture	bot*		
CreateResourcePolicy	Accorde l'autorisation de créer une politique de ressource pour une ressource Lex	Écrire	bot		
			bot alias		
CreateResourcePolicyStatement	Accorde l'autorisation de créer une nouvelle déclaration de politique de ressources pour une ressource Lex	Écrire	bot		
			bot alias		
CreateSlot	Accorde l'autorisation de créer un nouvel emplacement dans une intention	Écriture	bot*		
CreateSlotType	Accorde l'autorisation pour créer un nouveau type d'emplacement dans une locale de robot existante	Écrire	bot*		
CreateTestSet [autorisation uniquement]	Accorde l'autorisation d'importer un nouvel ensemble de tests	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTestSetDiscrepancyReport	Accorde l'autorisation de créer un rapport de différences entre les ensembles de tests	Écrire	test set*		
CreateUploadUrl	Accorde l'autorisation de créer une URL de chargement pour le fichier d'importation	Écriture			
DeleteBot	Accorde l'autorisation de supprimer un robot existant	Écriture	bot*		lex:DeleteBotAlias lex:DeleteBotChannel lex:DeleteBotLocale lex:DeleteBotVersion lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			bot alias*		
DeleteBotAlias	Accorde l'autorisation de supprimer un alias de robot existant dans un robot	Écrire	bot alias*		
DeleteBotAnalyzerRecommendation	Accorde l'autorisation de supprimer une recommandation de l'analyseur de robots	Écrire	bot*		
DeleteBotChannel [autorisation uniquement]	Accorde l'autorisation de supprimer un canal de robot existant	Écriture	bot*		
DeleteBotLocale	Accorde l'autorisation de supprimer une locale de robot existante dans un robot	Écrire	bot*		lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
DeleteBotReplica	Autorise la suppression d'une réplique de bot existante	Écrire	bot*		
DeleteBotVersion	Accorde l'autorisation de supprimer une version de robot existante	Écrire	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCustomVocabulary	Accorde l'autorisation de supprimer un vocabulaire personnalisé existant dans une locale de robot	Écrire	bot*		
DeleteExport	Accorde l'autorisation de supprimer une exportation existante	Écriture	bot		
			test set		
DeleteImport	Accorde l'autorisation de supprimer une importation existante	Écriture	bot		
			test set		
DeleteIntent	Accorde l'autorisation de supprimer une intention existante dans une locale de robot	Écriture	bot*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource existante pour une ressource Lex	Écrire	bot		
			bot alias		
DeleteResourcePolicyStatement	Accorde l'autorisation de supprimer une déclaration de politique de ressources existante pour une ressource Lex	Écrire	bot		
			bot alias		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSession	Accorde l'autorisation de supprimer les informations de session d'un alias de robot et d'un ID utilisateur	Écriture	bot alias*		
DeleteSlot	Accorde l'autorisation de supprimer un emplacement existant dans une intention	Écriture	bot*		
DeleteSlotType	Accorde l'autorisation de supprimer un type d'emplacement existant dans une locale de robot	Écrire	bot*		
DeleteTestSet	Accorde l'autorisation de supprimer un ensemble de tests existant	Écrire	test set*		
DeleteUtterances	Accorde l'autorisation de supprimer des données d'énoncé d'un bot	Écrire	bot*		
DescribeBot	Accorde l'autorisation de récupérer un robot existant	Lecture	bot*		
DescribeBotAlias	Accorde l'autorisation de récupérer un alias de robot existant	Lecture	bot alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeBotAnalyzerRecommendation	Accorde l'autorisation de décrire une recommandation d'un analyseur de robots	Lecture	bot*		
DescribeBotChannel [autorisation uniquement]	Accorde l'autorisation de récupérer un canal de robot existant	Lecture	bot*		
DescribeBotLocale	Accorde l'autorisation de récupérer une locale de robot existante	Lecture	bot*		
DescribeBotRecommendation	Accorde l'autorisation de récupérer des informations de métadonnées sur une recommandation de bot	Lecture	bot*		
DescribeBotReplica	Autorise la récupération d'une réplique de bot existante	Lecture	bot*		
DescribeBotResourceGeneration	Accorde l'autorisation de récupérer des informations de métadonnées pour une génération de ressource de bot	Lecture	bot*		
DescribeBotVersion	Accorde l'autorisation de récupérer une version de bot existante.	Lecture	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCustomVocabulary [autorisation uniquement]	Accorde l'autorisation de récupérer un vocabulaire personnalisé existant	Lecture	bot*		
DescribeCustomVocabularyMetadata	Accorde l'autorisation de récupérer les métadonnées d'un vocabulaire personnalisé existant	Lecture	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeExport	Accorde l'autorisation de récupérer une exportation existante	Lecture	bot		lex:DescribeBot lex:DescribeBotLocale lex:DescribeIntent lex:DescribeSlot lex:DescribeSlotType lex:ListBotLocales lex:ListIntents lex:ListSlotTypes lex:ListSlots
			test set		
DescribeImport		Lecture	bot		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de récupérer une importation existante		test set		
DescribeIntent	Accorde l'autorisation de récupérer une intention existante	Lecture	bot*		
DescribeResourcePolicy	Accorde l'autorisation de récupérer une politique de ressource existante pour une ressource Lex	Lecture	bot		
			bot alias		
DescribeSlot	Accorde l'autorisation de récupérer un emplacement existant	Lecture	bot*		
DescribeSlotType	Accorde l'autorisation de récupérer un type d'emplacement existant	Lecture	bot*		
DescribeTestExecution	Accorde l'autorisation de récupérer les métadonnées d'exécution des tests	Lecture	test set*		
DescribeTestSet	Accorde l'autorisation de récupérer un ensemble de tests existant	Lecture	test set*		
DescribeTestSetDiscrepancyReport	Accorde l'autorisation de récupérer les métadonnées du rapport de différences entre les ensembles de tests	Lecture	test set*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTestSetGeneration	Accorde l'autorisation de récupérer les métadonnées de génération de l'ensemble de tests	Lecture	test set		
GenerateBotElement	Accorde l'autorisation de générer des champs ou des éléments pris en charge pour un bot	Lecture	bot*		
GetSession	Accorde l'autorisation de récupérer des informations de session pour un alias de robot et un ID utilisateur	Lecture	bot alias*		
GetTestExecutionArtifactsUrl	Accorde l'autorisation de récupérer l'URL des artefacts pour l'exécution d'un test	Lecture	test set*		
ListAggregatedUtterances	Accorde l'autorisation de répertorier les énoncés et les statistiques d'un bot	List	bot*		
ListBotAliasReplicas	Octroie l'autorisation de répertorier les répliques d'alias dans une réplique de bot	List	bot*		
ListBotAliases	Accorde l'autorisation de répertorier des alias de bot dans un bot	List	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBotAnalyzerRecommendations	Accorde l'autorisation de répertorier les recommandations de l'analyseur de robots	List	bot*		
ListBotChannels [autorisation uniquement]	Accorde l'autorisation de répertorier les canaux de robots	Liste	bot*		
ListBotLocales	Accorde l'autorisation de répertorier locales de robot dans un robot	List	bot*		
ListBotRecommendations	Accorde l'autorisation d'obtenir une liste de recommandations de bot répondant aux critères spécifiés	List	bot*		
ListBotReplicas	Accorde l'autorisation de répertorier les répliques d'un bot	List	bot*		
ListBotResourceGenerations	Accorde l'autorisation de répertorier les générations de ressource pour un bot	List	bot*		
ListBotVersionReplicas	Accorde l'autorisation de répertorier les répliques de versions dans une réplique de bot	List	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBotVersions	Accorde l'autorisation de répertorier des versions de robots existantes	Liste	bot*		
ListBots	Accorde l'autorisation de répertorier les robots existants	Liste			
ListBuiltInIntents	Accorde l'autorisation de répertorier des intentions intégrées	Liste			
ListBuiltInSlotTypes	Accorde l'autorisation de répertorier des types d'emplacements intégrés	List			
ListCustomVocabularyItems	Accorde l'autorisation de répertorier les éléments d'un vocabulaire personnalisé existant	List	bot*		
ListExports	Accorde l'autorisation de répertorier des exportations existantes	Liste			
ListImports	Accorde l'autorisation de répertorier des importations existantes	List			
ListIntentMetrics	Octroie l'autorisation de répertorier les métriques d'analyse des intentions d'un bot.	List	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIntentPaths	Octroie l'autorisation de répertorier les analyses de chemin d'intention d'un bot.	List	bot*		
ListIntentStageMetrics	Octroie l'autorisation de répertorier les métriques d'analyse intentStage d'un bot.	List	bot*		
ListIntents	Accorde l'autorisation de répertorier des intentions dans un robot	List	bot*		
ListRecommendedIntents	Accorde l'autorisation d'obtenir une liste d'intentions recommandées fournie par la recommandation de bot	List	bot*		
ListSessionAnalyticsData	Octroie l'autorisation de répertorier les données d'analyse de session d'un bot.	List	bot*		
ListSessionMetrics	Octroie l'autorisation de répertorier les métriques d'analyse de session d'un bot.	List	bot*		
ListSlotTypes	Accorde l'autorisation de répertorier des types d'emplacements dans un robot	Liste	bot*		
ListSlots	Accorde l'autorisation de répertorier des emplacements dans une intention	Liste	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour une ressource Lex	Lecture	bot		
			bot alias		
			test set		
ListTestExecutionResultItems	Accorde l'autorisation de récupérer les données des résultats des tests pour une exécution de tests	Lecture	test set*		lex:ListTestSetRecords
ListTestExecutions	Accorde l'autorisation de répertorier les exécutions de tests	List			
ListTestSetRecords	Accorde l'autorisation de récupérer des enregistrements à l'intérieur d'un ensemble de tests existant	Lecture	test set*		
ListTestSets	Accorde l'autorisation de répertorier les ensembles de tests	List			
PutSession	Accorde l'autorisation de créer une nouvelle session ou modifier une session existante pour un alias de robot et un ID utilisateur	Écrire	bot alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RecognizeText	Accorde l'autorisation d'envoyer des entrées utilisateur (texte uniquement) à un alias de robot	Écrire	bot alias*		
RecognizeUtterance	Accorde l'autorisation d'envoyer une entrée utilisateur (texte ou parole) à un alias de robot	Écrire	bot alias*		
SearchAssociatedTranscripts	Accorde l'autorisation de rechercher des transcriptions associées répondant aux critères spécifiés	List	bot*		
StartBotAnalyzer	Autorise le démarrage d'un analyseur de bots pour un environnement de bot existant	Écrire	bot*		
StartBotRecommendation	Accorde l'autorisation de démarrer une recommandation de bot pour une locale de bot existante	Écrire	bot*		
StartBotResourceGeneration	Accorde l'autorisation de démarrer une génération de ressource pour une locale de bot existante	Écrire	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartConversation	Accorde l'autorisation de diffuser l'entrée utilisateur (speech/text/DTMF) à un alias de bot	Écrire	bot alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartImport	Accorde l'autorisation de démarrer une nouvelle importation avec le fichier d'importation téléchargé	Écrire	bot		lex:CreateBot lex:CreateBotLocale lex:CreateCustomVocabulary lex:CreateIntent lex:CreateSlot lex:CreateSlotType lex:CreateTestSet lex:DeleteBotLocale lex:DeleteCustomVocabulary lex:DeleteIntent

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					lex:DeleteSlot lex:DeleteSlotType lex:UpdateBot lex:UpdateBotLocale lex:UpdateCustomVocabulary lex:UpdateIntent lex:UpdateSlot lex:UpdateSlotType lex:UpdateTestSet
			bot alias		
			test set		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
StartTestExecution	Accorde l'autorisation de démarrer l'exécution d'un test à l'aide d'un ensemble de tests	Écrire	test set*		
StartTestSetGeneration	Accorde l'autorisation de générer un ensemble de tests	Écrire	test set		
StopBotAnalyzer	Autorise l'arrêt d'un analyseur de bot pour un environnement de bot existant	Écrire	bot*		
StopBotRecommendation	Accorde l'autorisation de démarrer une recommandation de bot pour une locale de bot existante	Écrire	bot*		
TagResource	Accorde l'autorisation d'ajouter ou d'écraser les balises d'une ressource Lex	Balisage	bot		
			bot alias		
			test set		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource Lex	Balisage	bot		
			bot alias		
			test set		
				aws:TagKeys	
UpdateBot	Accorde l'autorisation de mettre à jour un robot existant	Écriture	bot*		
UpdateBotAlias	Accorde l'autorisation de mettre à jour un alias de robot existant	Écriture	bot alias*		
UpdateBotLocale	Accorde l'autorisation de mettre à jour une locale de robot existante	Écrire	bot*		
UpdateBotRecommendation	Accorde l'autorisation de mettre à jour une demande de recommandation de bot existante	Écrire	bot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCustomVocabulary [autorisation uniquement]	Accorde l'autorisation de mettre à jour un vocabulaire personnalisé existant	Écrire	bot*		
UpdateExport	Accorde l'autorisation de mettre à jour une exportation existante	Écriture	bot*		
UpdateIntent	Accorde l'autorisation de mettre à jour une intention existante	Écriture	bot*		
UpdateResourcePolicy	Accorde l'autorisation de mettre à jour une politique de ressource existante pour une ressource Lex	Écriture	bot		
			bot alias		
UpdateSlot	Accorde l'autorisation de mettre à jour un emplacement existant	Écriture	bot*		
UpdateSlotType	Accorde l'autorisation de mettre à jour un type d'emplacement existant	Écrire	bot*		
UpdateTestSet	Accorde l'autorisation de mettre à jour un ensemble de tests existant	Écrire	test set*		

Types de ressources définis par Amazon Lex V2

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
bot	`arn:${Partition}:lex:${Region}:${Account}:bot/${BotId}`	aws:ResourceTag/${TagKey}
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot-alias/${BotId}/${BotAliasId}`	aws:ResourceTag/${TagKey}
test set	`arn:${Partition}:lex:${Region}:${Account}:test-set/${TestSetId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Lex V2

Amazon Lex V2 définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises de la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource Lex	String
aws:TagKeys	Filtre l'accès en fonction de l'ensemble des clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS License Manager

AWS License Manager (préfixe de service :`license-manager`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS License Manager
- Types de ressources définis par AWS License Manager
- Clés de condition pour AWS License Manager

Actions définies par AWS License Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptGrant	Accorde l'autorisation d'accepter un octroi	Écriture	grant*		
CheckInLicense	Accorde l'autorisation de réintégrer les droits de licence dans un pool	Écriture			
CheckoutBorrowLicense	Accorde l'autorisation d'extraire les droits de licence d'un cas d'utilisation d'emprunt	Écriture	license*		
CheckoutLicense	Accorde l'autorisation d'extraire les droits de licence	Écriture			
CreateGrant	Accorde l'autorisation de créer un nouvel octroi pour la licence	Écriture	license*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGrantVersion	Accorde l'autorisation de créer une version d'octroi	Écriture	grant*		
CreateLicense	Accorde l'autorisation de créer une licence	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLicenseAssetGroup	Accorde l'autorisation de créer un groupe d'actifs de licence	Écrire	license-asset-ruleset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseAssetRuleset	Accorde l'autorisation de créer un ensemble de règles relatives aux actifs de licence	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConfiguration	Accorde l'autorisation de créer une configuration de licence	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConversionTaskForResource	Accorde l'autorisation de créer une tâche de conversion de licence pour une ressource	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLicenseManagerReportGenerator	Autorise la création d'un générateur de rapports pour les ressources du gestionnaire de licences prises en charge	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseVersion	Accorde l'autorisation de créer une version de licence	Écrire	license*		
CreateToken	Accorde l'autorisation de créer un jeton de licence	Écrire	license*		
DeleteGrant	Accorde l'autorisation de supprimer un octroi d'autorisation (grant)	Écrire	grant*		
DeleteLicense	Accorde l'autorisation de supprimer une licence	Écrire	license*		
DeleteLicenseAssetGroup	Autorise la suppression d'un groupe de ressources de licence	Écrire	license-asset-group*		
DeleteLicenseAssetRuleset	Accorde l'autorisation de supprimer un ensemble de règles relatives aux actifs de licence	Écrire	license-asset-ruleset*		
DeleteLicenseConfiguration	Accorde l'autorisation de supprimer définitivement une configuration de licence	Écriture	license-configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLicenseManagerReportGenerator	Accorde l'autorisation de supprimer un générateur de rapports	Écriture	report-generator*		
DeleteToken	Accorde l'autorisation de supprimer un jeton	Écriture			
ExtendLicenseConsumption	Accorde l'autorisation de prolonger la période de consommation des droits de licence déjà extraits	Écriture			
GetAccessToken	Accorde l'autorisation d'obtenir un jeton d'accès	Lecture			
GetGrant	Accorde l'autorisation d'obtenir un octroi	Lecture	grant*		
GetLicense	Accorde l'autorisation d'obtenir une licence	Lecture	license*		
GetLicenseAssetGroup	Accorde l'autorisation d'obtenir un groupe d'actifs de licence	Lecture	license-asset-group*		
GetLicenseAssetRuleset	Accorde l'autorisation d'obtenir un ensemble de règles relatives aux actifs de licence	Lecture	license-asset-ruleset*		
GetLicenseConfiguration	Accorde l'autorisation d'obtenir une configuration de licence	Lecture	license-configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLicenseConversionTask	Accorde l'autorisation de récupérer une tâche de conversion de licence	Lecture			
GetLicenseManagerReportGenerator	Accorde l'autorisation d'obtenir un générateur de rapports	Lecture	report-generator*		
GetLicenseUsage	Accorde l'autorisation d'obtenir une utilisation de licence	Lecture	license*		
GetServiceSettings	Accorde l'autorisation d'obtenir les paramètres de service	List			
ListAssetsForLicenseAssetGroup	Accorde l'autorisation de répertorier les actifs d'un groupe d'actifs de licence	List	license-asset-group*		
ListAssociationsForLicenseConfiguration	Accorde l'autorisation de répertorier les associations d'une configuration de licence sélectionnée	Liste	license-configuration*		
ListDistributedGrants	Accorde l'autorisation de répertorier les octrois attribués	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFailuresForLicenseConfigurationOperations	Accorde l'autorisation de répertorier les opérations de configuration de licence ayant échoué	List	license-configuration*		
ListLicenseAssetGroups	Accorde l'autorisation de répertorier les groupes d'actifs de licence	List	license-asset-group		
ListLicenseAssetRulesets	Accorde l'autorisation de répertorier les ensembles de règles relatifs aux actifs de licence	List	license-asset-ruleset		
ListLicenseConfigurations	Accorde l'autorisation de répertorier les configurations de licence	List			
ListLicenseConfigurationsForOrganization	Accorde l'autorisation de répertorier les configurations de licence pour l'organisation	List			
ListLicenseConversionTasks	Accorde l'autorisation de répertorier les tâches de conversion de licence	List			
ListLicenseManagerReportGenerators	Accorde l'autorisation de répertorier les générateurs de rapports	Liste	license-configuration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLicenseSpecificationsForResource	Accorde l'autorisation de répertorier les spécifications de licence associées à une ressource sélectionnée	Liste			
ListLicenseVersions	Accorde l'autorisation de répertorier les versions d'une licence	Liste	license*		
ListLicenses	Accorde l'autorisation de répertorier les licences	Lecture			
ListReceivedGrants	Accorde l'autorisation de répertorier les octrois reçus	List			
ListReceivedGrantsForOrganization	Accorde l'autorisation de répertorier les octrois reçus pour l'organisation	List			
ListReceivedLicenses	Accorde l'autorisation de répertorier les licences reçues	List			
ListReceivedLicensesForOrganization	Accorde l'autorisation de répertorier les licences reçues pour l'organisation	List			
ListResourceInventory	Accorde l'autorisation de répertorier un inventaire de ressources	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource sélectionnée	Lecture	grant		
			license		
			license-asset-group		
			license-asset-ruleset		
			license-configuration		
			report-generator		
ListTokens	Accorde l'autorisation de répertorier les jetons	Liste			
ListUsageForLicenseConfiguration	Accorde l'autorisation de répertorier les enregistrements d'utilisation d'une configuration de licence sélectionnée	Liste	license-configuration*		
RejectGrant	Accorde l'autorisation de rejeter un octroi	Écriture	grant*		
TagResource	Accorde l'autorisation de baliser une ressource sélectionnée	Balisage	grant		
			license		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			license-asset-group		
			license-asset-ruleset		
			license-configuration		
			report-generator		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource sélectionnée	Identification	grant		
			license		
			license-asset-group		
			license-asset-ruleset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			license-configuration		
			report-generator		
				aws:TagKeys	
UpdateLicenseAssetGroup	Autorise la mise à jour d'un groupe d'actifs de licence	Écrire	license-asset-group*		
			license-asset-ruleset*		
UpdateLicenseAssetRuleset	Autorise la mise à jour d'un ensemble de règles relatives aux actifs de licence	Écrire	license-asset-ruleset*		
UpdateLicenseConfiguration	Accorde l'autorisation de mette à jour une configuration de licence existante	Écrire	license-configuration*		
UpdateLicenseManagerReportGenerator	Autorise la mise à jour d'un générateur de rapports pour les ressources du gestionnaire de licences prises en charge	Écrire	report-generator*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateLicenseSpecificationsForResource	Accorde l'autorisation de mettre à jour les spécifications de licence d'une ressource sélectionnée	Écriture	license-configuration*		
UpdateServiceSettings	Accorde l'autorisation de mettre à jour les paramètres d'un service	Gestion des autorisations			

Types de ressources définis par AWS License Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
license-configuration	`arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}`	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}
license	`arn:${Partition}:license-manager::${Account}:license:${LicenseId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
grant	arn:${Partition}:license-manager::${Account}:grant:${GrantId}	aws:ResourceTag/${TagKey}
report-generator	arn:${Partition}:license-manager:${Region}:${Account}:report-generator:${ReportGeneratorId}	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}
license-asset-ruleset	arn:${Partition}:license-manager:${Region}:${Account}:license-asset-ruleset:${LicenseAssetRulesetId}	aws:ResourceTag/${TagKey}
license-asset-group	arn:${Partition}:license-manager:${Region}:${Account}:license-asset-group:${LicenseAssetGroupId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS License Manager

AWS License Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString
license-manager:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String

Actions, ressources et clés de condition pour AWS License Manager Linux Subscriptions Manager

AWS License Manager Linux Subscriptions Manager (préfixe de service :`license-manager-linux-subscriptions`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS License Manager Linux Subscriptions Manager
- Types de ressources définis par AWS License Manager Linux Subscriptions Manager
- Clés de condition pour AWS License Manager Linux Subscriptions Manager

Actions définies par AWS License Manager Linux Subscriptions Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterSubscriptionProvider	Accorde l'autorisation de supprimer définitivement un fournisseur d'abonnement dans AWS License Manager	Écrire	subscription-provider*		
GetRegisteredSubscriptionProvider	Accorde l'autorisation d'obtenir un fournisseur d'abonnement dans AWS License Manager	Lecture	subscription-provider*		
GetServiceSettings	Accorde l'autorisation d'obtenir les paramètres de service pour les abonnements Linux dans AWS License Manager	Lecture			
ListLinuxSubscriptionInstances	Accorde l'autorisation de répertorier toutes les instances avec des abonnements Linux dans AWS License Manager	Lecture			
ListLinuxSubscriptions	Accorde l'autorisation de répertorier tous les abonnements Linux dans AWS License Manager	Lecture			
ListRegisteredSubscriptionProviders	Accorde l'autorisation de répertorier les fournisseurs d'abonnement dans AWS License Manager	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource sélectionnée	Lecture	subscription-provider*		
RegisterSubscriptionProvider	Autorise la création d'un nouveau fournisseur d'abonnement dans AWS License Manager	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation de baliser une ressource sélectionnée	Balisage	subscription-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource sélectionnée	Identification	subscription-provider*		
				aws:TagKeys	
UpdateServiceSettings	Autorise la mise à jour des paramètres de service pour les abonnements Linux dans AWS License Manager	Écrire			

Types de ressources définis par AWS License Manager Linux Subscriptions Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
subscription-provider	`arn:${Partition}:license-manager-linux-subscriptions:${Region}:${Account}:subscription-provider/${SubscriptionProviderId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS License Manager Linux Subscriptions Manager

AWS License Manager Linux Subscriptions Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les abonnements utilisateurs AWS de License Manager

AWS License Manager User Subscriptions (préfixe de service :`license-manager-user-subscriptions`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS License Manager User Subscriptions
- Types de ressources définis par AWS License Manager User Subscriptions
- Clés de condition pour les abonnements utilisateurs de AWS License Manager

Actions définies par AWS License Manager User Subscriptions

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateUser	Accorde l'autorisation d'associer un utilisateur abonné à une instance lancée avec les produits à abonnements utilisateur de License Manager	Écrire	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseServerEndpoint	Accorde l'autorisation de créer un point de terminaison de serveur de licences pour un type de serveur donné pour un fournisseur d'identité donné	Écrire	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLicenseServerEndpoint	Accorde l'autorisation de supprimer un point de terminaison de serveur de licences pour un type de serveur donné pour un fournisseur d'identité donné	Écrire	identity-provider*		
			license-server-endpoint*		
DeregisterIdentityProvider	Accorde l'autorisation de désenregistrer Microsoft Active Directory license-manager-user-subscriptions pour un produit	Écrire	identity-provider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateUser	Accorde l'autorisation de dissocier un utilisateur abonné d'une instance lancée avec les produits à abonnements utilisateur de License Manager	Écrire	identity-provider*		
			instance-user*		
ListIdentityProviders	Accorde l'autorisation de répertorier tous les fournisseurs d'identité des abonnements utilisateur de License Manager	List			
ListInstances	Accorde l'autorisation de répertorier toutes les instances lancées avec des produits à abonnements utilisateur de License Manager	List			
ListLicenseServerEndpoints	Accorde l'autorisation de répertorier les points de terminaison du serveur de licences	List			
ListProductSubscriptions	Accorde l'autorisation de répertorier tous les abonnements de produits pour un produit et un fournisseur d'identité	List	identity-provider*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource sélectionnée	Lecture	identity-provider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
ListUserAssociations	Accorde l'autorisation de répertorier tous les utilisateurs associés à une instance lancée pour un produit	List	identity-provider*		
RegisterIdentityProvider	Accorde l'autorisation d'enregistrer Microsoft Active Directory auprès license-manager-user-subscriptions d'un produit	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
StartProductSubscription	Accorde l'autorisation de démarrer l'abonnement au produit pour un utilisateur sur un Active Directory enregistré pour un produit	Écrire	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopProductSubscription	Accorde l'autorisation d'arrêter l'abonnement au produit pour un utilisateur sur un Active Directory enregistré pour un produit	Écrire	identity-provider*		
			product-subscription*		
TagResource	Accorde l'autorisation de baliser une ressource sélectionnée	Balisage	identity-provider*		
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource sélectionnée	Identification	identity-provider*		
			instance-user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			license-server-endpoint*		
			product-subscription*		
UpdateIdentityProviderSettings	Accorde l'autorisation de mettre à jour la configuration du fournisseur d'identité	Écrire	identity-provider*		

Types de ressources définis par AWS License Manager User Subscriptions

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
identity-provider	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:identity-provider/${IdentityProviderId}`	aws:ResourceTag/${TagKey}
product-subscription	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
	`:product-subscription/${ProductSubscriptionId}`	
instance-user	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:instance-user/${InstanceUserId}`	aws:ResourceTag/${TagKey}
license-server-endpoint	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:license-server-endpoint/${LicenseServerEndpointId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les abonnements utilisateurs de AWS License Manager

AWS License Manager User Subscriptions définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Lightsail

Amazon Lightsail (préfixe de service : `lightsail`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Lightsail
- Types de ressources définis par Amazon Lightsail
- Clés de condition pour Amazon Lightsail

Actions définies par Amazon Lightsail

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllocateStaticIp	Accorde l'autorisation de créer une adresse IP statique qui peut être attachée à une instance	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AttachCertificateToDistribution	Accorde l'autorisation de joindre un SSL/TLS certificat à votre réseau de diffusion de contenu (CDN) Amazon Lightsail	Écrire	Certificate*		
			Distribution*		
AttachDisk	Accorde l'autorisation d'attacher un disque à une instance	Écriture	Disk*		
AttachInstancesToLoadBalancer	Accorde l'autorisation d'attacher une ou plusieurs instances à un équilibreur de charge	Écriture	LoadBalancer*		
AttachLoadBalancerTlsCertificate	Accorde l'autorisation d'attacher un certificat TLS à un équilibreur de charge	Écriture	LoadBalancer*		
AttachStaticIp	Accorde l'autorisation d'attacher une adresse IP statique à une instance	Écriture	Instance*		
			StaticIp*		
CloseInstancePublicPorts	Accorde l'autorisation de fermer un port public d'une instance	Écrire	Instance*		
CopySnapshot	Autorise la copie d'un instantané de l'un Région AWS à l'autre dans Amazon Lightsail	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBucket	Accorde l'autorisation de créer un conteneur Amazon Lightsail	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBucketAccessKey	Accorde l'autorisation de créer une clé d'accès pour le conteneur spécifié	Écrire	Bucket*		
CreateCertificate	Accorde l'autorisation de créer un SSL/TLS certificat	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains
CreateCloudFormationStack	Accorde l'autorisation de créer une nouvelle instance Amazon EC2 à partir d'un instantané Amazon Lightsail exporté	Écriture			
CreateContactMethod	Accorde l'autorisation de créer une méthode de contact par e-mail ou SMS.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateContainerService	Accorde l'autorisation de créer un service de conteneur Amazon Lightsail.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContainerServiceDeployment	Accorde l'autorisation de créer un déploiement pour votre service de conteneur Amazon Lightsail.	Écriture	ContainerService*		
CreateContainerServiceRegistryLogin	Accorde l'autorisation de créer un jeu temporaire d'informations d'identification de connexion que vous pouvez utiliser pour vous connecter au processus Docker sur votre ordinateur local.	Écriture			
CreateDisk	Accorde l'autorisation de créer un disque	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskFromSnapshot	Accorde l'autorisation de créer un disque à partir d'un instantané	Écriture	DiskSnapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskSnapshot	Accorde l'autorisation de créer un instantané de disque	Écriture	Disk Instance		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDistribution	Accorde l'autorisation de créer une distribution de réseau de diffusion de contenu (CDN) Amazon Lightsail.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDomain	Accorde l'autorisation de créer une ressource de domaine pour le domaine spécifié	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	route53:DeleteHostedZone route53:GetHostedZone route53:ListHostedZonesByName route53domains:GetDomainDetail route53domains:GetOperationDetail route53domains:ListDomains route53domains:ListOperations

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					route53domains:UpdateDomainNameservers
CreateDomainEntry	Accorde l'autorisation de créer une ou plusieurs entrées d'enregistrement DNS pour une ressource de domaine : adresse (A), nom canonique (CNAME), échangeur de messagerie (MX), serveur de noms (NS), start of authority (SOA), localisateur de service (SRV) ou texte (TXT).	Écrire	Domain*		
CreateGUISessionAccessDetails	Accorde l'autorisation de créer URLs des informations utilisées pour accéder à la session d'interface utilisateur graphique (GUI) d'une instance	Écrire	Instance*		
CreateInstanceSnapshot	Accorde l'autorisation de créer un instantané d'instance	Écriture	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInstances	Accorde l'autorisation de créer une ou plusieurs instances.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInstancesFromSnapshot	Accorde l'autorisation de créer une ou plusieurs instances en fonction d'un instantané d'instance	Écriture	InstanceSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeyPair	Accorde l'autorisation de créer une paire de clés utilisée pour s'authentifier et se connecter à une instance	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoadBalancer	Accorde l'autorisation de créer un équilibreur de charge	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLoadBalancerTlsCertificate	Accorde l'autorisation de créer un certificat SSL/TLS d'équilibreur de charge	Écriture	LoadBalancer*		lightsail:CreateDomainEntry lightsail:GetDomains
CreateRelationalDatabase	Accorde l'autorisation de créer une base de données relationnelle	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseFromSnapshot	Accorde l'autorisation de créer une base de données relationnelle à partir d'un instantané	Écriture	RelationalDatabaseSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseSnapshot	Accorde l'autorisation de créer un instantané de base de données relationnelle	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAlarm	Accorde l'autorisation de supprimer une alarme.	Écriture	Alarm*		
DeleteAutoSnapshot	Accorde l'autorisation de supprimer un instantané automatique d'une instance ou d'un disque.	Écriture			
DeleteBucket	Accorde l'autorisation de supprimer un compartiment Amazon Lightsail	Écriture	Bucket*		
DeleteBucketAccessKey	Accorde l'autorisation de supprimer une clé d'accès pour le compartiment Amazon Lightsail spécifié	Écrire	Bucket*		
DeleteCertificate	Accorde l'autorisation de supprimer un SSL/TLS certificat	Écrire	Certificate*		
DeleteContactMethod	Accorde l'autorisation de supprimer une méthode de contact.	Écriture			
DeleteContainerImage	Accorde l'autorisation de supprimer une image de conteneur enregistrée sur votre service de conteneur Amazon Lightsail.	Écriture	ContainerService*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteContainerService	Accorde l'autorisation de supprimer votre service de conteneur Amazon Lightsail.	Écriture	ContainerService*		
DeleteDisk	Accorde l'autorisation de supprimer un disque	Écriture	Disk*		
DeleteDiskSnapshot	Accorde l'autorisation de supprimer un instantané de disque	Écriture	DiskSnapshot*		
DeleteDistribution	Accorde l'autorisation de supprimer votre distribution de réseau de diffusion de contenu (CDN) Amazon Lightsail.	Écriture	Distribution*		
DeleteDomain	Accorde l'autorisation de supprimer une ressource de domaine et tous ses enregistrements DNS	Écriture	Domain*		
DeleteDomainEntry	Accorde l'autorisation de supprimer une entrée d'enregistrement DNS pour une ressource de domaine	Écriture	Domain*		
DeleteInstance	Accorde l'autorisation de supprimer une instance	Écriture	Instance*		
DeleteInstanceSnapshot	Accorde l'autorisation de supprimer un instantané d'instance	Écriture	InstanceSnapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteKeyPair	Accorde l'autorisation de supprimer une paire de clés utilisée pour s'authentifier et se connecter à une instance	Écriture	KeyPair*		
DeleteKnownHostKeys	Accorde l'autorisation de supprimer la clé d'hôte connue ou le certificat utilisé par les clients SSH ou RDP basés sur un navigateur Amazon Lightsail pour authentifier une instance	Écriture	Instance*		
DeleteLoadBalancer	Accorde l'autorisation de supprimer un équilibreur de charge	Écriture	LoadBalancer*		
DeleteLoadBalancerTlsCertificate	Accorde l'autorisation de supprimer un certificat SSL/TLS d'équilibreur de charge	Écriture	LoadBalancer*		
DeleteRelationalDatabase	Accorde l'autorisation de supprimer une base de données relationnelle	Écriture	RelationalDatabase*		
DeleteRelationalDatabaseSnapshot	Accorde l'autorisation de supprimer un instantané de base de données relationnelle	Écrire	RelationalDatabaseSnapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DetachCertificateFromDistribution	Autorise le détachement d'un SSL/TLS certificat de votre réseau de diffusion de contenu (CDN) Amazon Lightsail	Écrire	Distribution*		
DetachDisk	Accorde l'autorisation de détacher un disque d'une instance	Écriture	Disk*		
DetachInstancesFromLoadBalancer	Accorde l'autorisation de détacher une ou plusieurs instances d'un équilibreur de charge	Écriture	LoadBalancer*		
DetachStaticIp	Accorde l'autorisation de détacher une adresse IP statique d'une instance à laquelle elle est attachée	Écriture	StaticIp*		
DisableAddOn	Accorde l'autorisation de désactiver un module complémentaire pour une ressource Amazon Lightsail.	Écrire			
DownloadDefaultKeyPair	Accorde l'autorisation de télécharger la paire de clés par défaut utilisée pour authentifier et se connecter aux instances d'un Région AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableAddOn	Accorde l'autorisation d'activer ou de modifier un module complémentaire pour une ressource Amazon Lightsail.	Écriture			
ExportSnapshot	Accorde l'autorisation d'exporter un instantané Amazon Lightsail vers Amazon EC2	Écriture	DiskSnapshot		iam:CreateServiceLinkedRole iam:PutRolePolicy
			InstanceSnapshot		
GetActiveNames	Accorde l'autorisation d'obtenir les noms de toutes les ressources actives (non supprimées)	Lecture			
GetAlarms	Accorde l'autorisation d'afficher des informations sur les alarmes configurées.	Lecture			
GetAutoSnapshots	Accorde l'autorisation d'afficher les instantanés automatiques disponibles pour une instance ou un disque.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBlueprints	Accorde l'autorisation d'obtenir une liste d'images d'instance, ou plans. Un plan vous permet de créer une instance exécutant déjà un système d'exploitation spécifique, ainsi qu'une application ou une pile de développement préinstallée. Le logiciel qui s'exécute sur votre instance dépend du plan que vous définissez lors de la création de l'instance.	Lecture			
GetBucketAccessKeys	Accorde l'autorisation d'obtenir la clé d'accès existante IDs pour le bucket Amazon Lightsail spécifié	Lecture			
GetBucketBundles	Accorde l'autorisation d'obtenir les solutions groupées qui peuvent être appliquées à un compartiment Amazon Lightsail	Lecture			
GetBucketMetricData	Accorde l'autorisation d'obtenir les points de données d'une métrique spécifique pour un compartiment Amazon Lightsail	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBuckets	Accorde l'autorisation d'afficher les informations sur un ou plusieurs compartiments Amazon Lightsail	Lecture			
GetBundles	Accorde l'autorisation d'obtenir une liste d'ensemble d'instances Vous pouvez utiliser un groupe pour créer une instance avec un ensemble de spécifications de performances, telles que le nombre d'UC, la taille du disque, la taille de la RAM et l'allocation de transfert réseau. Le coût de votre instance dépend du groupe que vous définissez lors de la création de l'instance.	Lecture			
GetCertificates	Autorise l'accès aux informations relatives à un ou plusieurs certificats Amazon Lightsail SSL/TLS	Lecture			
GetCloudFormationStackRecords	Permet d'obtenir des informations sur toutes les CloudFormation piles utilisées pour créer des ressources Amazon EC2 à partir d'instantanés Amazon Lightsail exportés	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContactMethods	Accorde l'autorisation d'afficher des informations sur les méthodes de contact configurées.	Lecture			
GetContainerAPIMetadata	Accorde l'autorisation d'afficher des informations sur les conteneurs Amazon Lightsail, comme la version actuelle du plugin Lightsail Control (lightsailctl).	Lecture			
GetContainerImages	Accorde l'autorisation d'afficher les images de conteneur enregistrées sur votre service de conteneur Amazon Lightsail.	Lecture			
GetContainerLog	Accorde l'autorisation d'afficher les événements de journal d'un conteneur de votre service de conteneur Amazon Lightsail.	Lecture			
GetContainerServiceDeployments	Accorde l'autorisation d'afficher les déploiements pour votre service de conteneur Amazon Lightsail.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContainerServiceMetricData	Accorde l'autorisation d'afficher les points de données d'une métrique spécifique de votre service de conteneur Amazon Lightsail.	Lecture			
GetContainerServicePowers	Accorde l'autorisation d'afficher la liste des pouvoirs qui peuvent être spécifiés pour vos services de conteneur Amazon Lightsail.	Lecture			
GetContainerServices	Accorde l'autorisation d'afficher des informations sur un ou plusieurs de vos services de conteneur Amazon Lightsail.	Lecture			
GetCostEstimate	Octroie l'autorisation d'obtenir des informations sur le coût estimé d'une ressource spécifiée	Lecture	Disk Instance		
GetDisk	Accorde les autorisations d'obtenir des informations sur un disque	Lecture			
GetDiskSnapshot	Accorde l'autorisation d'obtenir des informations sur un instantané de disque	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDiskSnapshots	Accorde l'autorisation d'obtenir des informations sur tous les instantanés de disque	Lecture			
GetDisks	Accorde l'autorisation d'obtenir des informations sur tous les disques	Lecture			
GetDistributionBundles	Accorde l'autorisation d'afficher la liste des groupes qui peuvent être appliqués à vos distributions de réseau de diffusion de contenu (CDN) Amazon Lightsail.	Lecture			
GetDistributionLatestCacheReset	Accorde l'autorisation d'afficher l'horodatage et l'état de la dernière réinitialisation du cache d'une distribution de réseau de diffusion de contenu (CDN) Amazon Lightsail spécifique.	Lecture			
GetDistributionMetricData	Accorde l'autorisation d'afficher les points de données d'une métrique spécifique pour une distribution de réseau de diffusion de contenu (CDN) Amazon Lightsail.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDistributions	Accorde l'autorisation d'afficher des informations sur une ou plusieurs de vos distributions de réseau de diffusion de contenu (CDN) Amazon Lightsail.	Lecture			
GetDomain	Accorde l'autorisation d'obtenir des enregistrements DNS pour une ressource de domaine	Lecture			
GetDomains	Accorde l'autorisation d'obtenir des enregistrements DNS pour toutes les ressources de domaine	Lecture			
GetExportSnapshotRecords	Renvoie des informations sur tous les enregistrements pour exporter des instantanés Amazon Lightsail vers Amazon EC2	Lecture			
GetInstance	Accorde l'autorisation d'obtenir des informations sur une instance	Lecture			
GetInstanceAccessDetails	Accorde l'autorisation d'obtenir des clés temporaires que vous pouvez utiliser pour vous authentifier et vous connecter à une instance	Écriture	Instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInstanceMetricData	Accorde l'autorisation d'obtenir les points de données pour la métrique spécifiée d'une instance	Lecture			
GetInstancePortStates	Accorde l'autorisation d'obtenir les états de port d'une instance	Lecture			
GetInstanceSnapshot	Accorde l'autorisation d'obtenir des informations sur un instantané d'instance	Lecture			
GetInstanceSnapshots	Accorde l'autorisation d'obtenir des informations sur tous les instantanés d'instance	Lecture			
GetInstanceState	Accorde l'autorisation d'obtenir l'état d'une instance	Lecture			
GetInstances	Accorde l'autorisation d'obtenir des informations sur toutes les instances	Lecture			
GetKeyPair	Accorde l'autorisation d'obtenir des informations sur une paire de clés	Lecture			
GetKeyPairs	Accorde l'autorisation d'obtenir des informations sur toutes les paires de clés	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLoadBalancer	Accorde l'autorisation d'obtenir des informations sur un équilibreur de charge	Lecture			
GetLoadBalancerMetricData	Accorde l'autorisation d'obtenir les points de données pour la métrique spécifiée d'un équilibreur de charge	Read			
GetLoadBalancerTlsCertificates	Accorde l'autorisation d'obtenir des informations sur les certificats TLS d'un équilibreur de charge	Lecture			
GetLoadBalancerTlsPolicies	Accorde l'autorisation d'obtenir une liste des politiques de sécurité TLS que vous pouvez appliquer aux équilibreurs de charge Lightsail	Lecture			
GetLoadBalancers	Accorde l'autorisation d'obtenir des informations sur des équilibreurs de charge	Read			
GetOperation	Accorde l'autorisation d'obtenir des informations sur une opération Les opérations incluent des événements tels que la création d'une instance, l'allocation d'une adresse IP statique, l'attachement d'une adresse IP statique, etc.	Read			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOperations	Accorde l'autorisation d'obtenir des informations sur toutes les opérations Les opérations incluent des événements tels que la création d'une instance, l'allocation d'une adresse IP statique, l'attachement d'une adresse IP statique, etc.	Read			
GetOperationsForResource	Accorde l'autorisation d'obtenir des opérations pour une ressource	Lecture			
GetRegions	Accorde l'autorisation d'obtenir une liste de toutes les applications valides Régions AWS pour Amazon Lightsail	Lecture			
GetRelationalDatabase	Accorde l'autorisation d'obtenir des informations sur une base de données relationnelle	Read			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRelationalDatabaseBlueprints	Accorde l'autorisation d'obtenir une liste d'images de base de données relationnelle, ou plans. Vous pouvez utiliser un plan pour créer une base de données exécutant un moteur de base de données spécifique. Le moteur de base de données qui s'exécute sur votre base de données dépend du plan que vous définissez lors de la création de la base de données relationnelle.	Read			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRelationalDatabaseBundles	Accorde l'autorisation d'obtenir une liste de solutions groupées de bases de données relationnelles Vous pouvez utiliser un groupe pour créer une base de données avec un ensemble de spécifications de performances, telles que le nombre d'UC, la taille du disque, la taille de la RAM, l'allocation de transfert réseau et la haute disponibilité. Le coût de votre base de données dépend du groupe que vous définissez lors de la création de la base de données relationnelle.	Read			
GetRelationalDatabaseEvents	Accorde l'autorisation d'obtenir les événements relatifs à une base de données relationnelle	Read			
GetRelationalDatabaseLogEvents	Accorde l'autorisation d'obtenir les événements pour le flux de journaux spécifié d'une base de données relationnelle	Read			
GetRelationalDatabaseLogStreams	Accorde l'autorisation d'obtenir les flux de journaux disponibles pour une base de données relationnelle	Read			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRelationalDatabaseMasterUserPassword	Accorde l'autorisation d'obtenir le mot de passe de l'utilisateur principal d'une base de données relationnelle	Écriture	RelationalDatabase*		
GetRelationalDatabaseMetricData	Accorde l'autorisation d'obtenir les points de données pour la métrique spécifiée d'une base de données relationnelle	Read			
GetRelationalDatabaseParameters	Accorde l'autorisation d'obtenir les paramètres d'une base de données relationnelle	Read			
GetRelationalDatabaseSnapshot	Accorde l'autorisation d'obtenir des informations sur un instantané de base de données relationnelle	Read			
GetRelationalDatabaseSnapshots	Accorde l'autorisation d'obtenir des informations sur tous les instantanés de base de données relationnelle	Read			
GetRelationalDatabases	Accorde l'autorisation d'obtenir des informations sur toutes les bases de données relationnelles	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSetupHistory	Accorde l'autorisation d'obtenir des informations détaillées pour les demandes de configuration exécutées sur la ressource spécifiée	Lecture	Instance		
GetStaticIp	Accorde l'autorisation d'obtenir des informations sur une adresse IP statique	Lecture			
GetStaticIps	Accorde l'autorisation d'obtenir des informations sur toutes les données statiques IPs	Lecture			
ImportKeyPair	Accorde l'autorisation d'importer une clé publique à partir d'une paire de clés	Écriture			
IsVpcPeered	Accorde l'autorisation d'obtenir une valeur booléenne indiquant si le Virtual Private Cloud (VPC) Amazon Lightsail est appairé	Read			
OpenInstancePublicPorts	Accorde l'autorisation d'ajouter ou d'ouvrir un port public sur une instance	Écriture	Instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PeerVpc	Accorde l'autorisation de tenter d'appairer le Virtual Private Cloud (VPC) Amazon Lightsail avec le VPC par défaut.	Écriture			
PutAlarm	Accorde l'autorisation de créer ou de mettre à jour une alarme et de l'associer à la métrique spécifiée.	Écriture	Alarm*		
PutInstancePublicPorts	Accorde l'autorisation de définir les ports ouverts spécifiés pour une instance et de fermer tous les ports pour chaque protocole non inclus dans la demande	Écriture	Instance*		
RebootInstance	Accorde l'autorisation de redémarrer une instance qui est en cours d'exécution	Écriture	Instance*		
RebootRelationalDatabase	Accorde l'autorisation de redémarrer une base de données relationnelle qui est en cours d'exécution	Écriture	RelationalDatabase*		
RegisterContainerImage	Accorde l'autorisation d'enregistrer une image de conteneur sur votre service de conteneur Amazon Lightsail.	Écriture	ContainerService*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ReleaseStaticIp	Accorde l'autorisation de supprimer une adresse IP statique	Écriture	StaticIp*		
ResetDistributionCache	Accorde l'autorisation de supprimer le contenu actuellement mis en cache de votre distribution de réseau de diffusion de contenu (CDN) Amazon Lightsail.	Écriture	Distribution*		
SendContactMethodVerification	Accorde l'autorisation d'envoyer une demande de vérification à une méthode de contact par e-mail pour s'assurer qu'elle appartient au demandeur.	Écriture			
SetIpAddressType	Accorde l'autorisation de définir le type d'adresse IP pour une ressource Amazon Lightsail.	Écriture	Distribution		
			Instance		
			LoadBalancer		
SetResourceAccessForBucket	Accorde l'autorisation de définir les ressources Amazon Lightsail qui peuvent accéder au compartiment Amazon Lightsail spécifié	Écrire	Bucket*		
			Instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetupInstanceHttps	Accorde l'autorisation de créer un SSL/TLS certificat et de l'installer sur une instance spécifiée	Écrire	Instance*		lightsail:GetInstanceAccessDetails
StartGUISession	Octroie l'autorisation de lancer une session d'interface utilisateur graphique (GUI) utilisée pour accéder au système d'exploitation ou à l'application d'une instance	Écrire	Instance*		
StartInstance	Accorde l'autorisation de démarrer une instance à l'état arrêté	Écriture	Instance*		
StartRelationalDatabase	Accorde l'autorisation de démarrer une base de données relationnelle qui est à l'état arrêté	Écrire	RelationalDatabase*		
StopGUISession	Octroie l'autorisation de résilier une session d'interface utilisateur graphique (GUI) utilisée pour accéder au système d'exploitation ou à l'application d'une instance	Écrire	Instance*		
StopInstance	Accorde l'autorisation d'arrêter une instance en cours d'exécution	Écriture	Instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopRelationalDatabase	Accorde l'autorisation d'arrêter une base de données relationnelle qui est en cours d'exécution	Écriture	RelationalDatabase*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	Bucket		
			Certificate		
			ContactMethod		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestAlarm	Accorde l'autorisation de tester une alarme en affichant une bannière sur la console Amazon Lightsail ou, si un déclencheur de notification est configuré pour l'alarme spécifiée, en envoyant une notification au protocole de notification.	Écriture	Alarm*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UnpeerVpc	Accorde l'autorisation de tenter d'annuler l'appairage d'un Virtual Private Cloud (VPC) Amazon Lightsail avec le VPC par défaut	Écriture			
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	Bucket		
			Certificate		
			ContactMethod		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:TagKeys	
UpdateBucket	Accorde l'autorisation de mettre à jour un compartiment Amazon Lightsail existant	Écriture	Bucket*		
UpdateBucketBundle	Accorde l'autorisation de mettre à jour la solution groupée, ou le plan de stockage, d'un compartiment Amazon Lightsail existant	Écriture	Bucket*		
UpdateContainerService	Accorde l'autorisation de mettre à jour la configuration de votre service de conteneur Amazon Lightsail, par exemple sa puissance, sa mise à l'échelle et ses noms de domaine public.	Écriture	ContainerService*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDistribution	Accorde l'autorisation de mettre à jour une distribution de réseau de diffusion de contenu (CDN) Amazon Lightsail existante ou sa configuration.	Écriture	Distribution*		
UpdateDistributionBundle	Accorde l'autorisation de mettre à jour le groupe de votre distribution de réseau de diffusion de contenu (CDN) Amazon Lightsail.	Écriture	Distribution*		
UpdateDomainEntry	Accorde l'autorisation de mettre à jour le jeu d'enregistrements d'un domaine après sa création	Écrire	Domain*		
UpdateInstanceMetadataOptions	Accorde l'autorisation de modifier les options de métadonnées d'une instance	Écrire	Instance*		
UpdateLoadBalancerAttribute	Accorde l'autorisation de mettre à jour un attribut d'équilibreur de charge, tel que le chemin d'accès à la surveillance de l'état et la permanence de session	Écriture	LoadBalancer*		
UpdateRelationalDatabase	Accorde l'autorisation de mettre à jour une base de données relationnelle	Écriture	RelationalDatabase*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRelationalDatabaseParameters	Accorde l'autorisation de mettre à jour les paramètres d'une base de données relationnelle	Écriture	RelationalDatabase*		

Types de ressources définis par Amazon Lightsail

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Domain	`arn:${Partition}:lightsail:${Region}:${Account}:Domain/${Id}`	aws:ResourceTag/${TagKey}
Instance	`arn:${Partition}:lightsail:${Region}:${Account}:Instance/${Id}`	aws:ResourceTag/${TagKey}
InstanceSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:InstanceSnapshot/${Id}`	aws:ResourceTag/${TagKey}
KeyPair	`arn:${Partition}:lightsail:${Region}:${Account}:KeyPair/${Id}`	aws:ResourceTag/${TagKey}
StaticIp	`arn:${Partition}:lightsail:${Region}:${Account}:StaticIp/${Id}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Disk	arn:${Partition}:lightsail:${Region}:${Account}:Disk/${Id}	aws:ResourceTag/${TagKey}
DiskSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:DiskSnapshot/${Id}	aws:ResourceTag/${TagKey}
LoadBalancer	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancer/${Id}	aws:ResourceTag/${TagKey}
LoadBalancerTlsCertificate	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancerTlsCertificate/${Id}	
ExportSnapshotRecord	arn:${Partition}:lightsail:${Region}:${Account}:ExportSnapshotRecord/${Id}	
CloudFormationStackRecord	arn:${Partition}:lightsail:${Region}:${Account}:CloudFormationStackRecord/${Id}	
RelationalDatabase	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabase/${Id}	aws:ResourceTag/${TagKey}
RelationalDatabaseSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabaseSnapshot/${Id}	aws:ResourceTag/${TagKey}
Alarm	arn:${Partition}:lightsail:${Region}:${Account}:Alarm/${Id}	
Certificate	arn:${Partition}:lightsail:${Region}:${Account}:Certificate/${Id}	aws:ResourceTag/${TagKey}
ContactMethod	arn:${Partition}:lightsail:${Region}:${Account}:ContactMethod/${Id}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Container Service	`arn:${Partition}:lightsail:${Region}:${Account}:ContainerService/${Id}`	aws:ResourceTag/${TagKey}
Distribution	`arn:${Partition}:lightsail:${Region}:${Account}:Distribution/${Id}`	aws:ResourceTag/${TagKey}
Bucket	`arn:${Partition}:lightsail:${Region}:${Account}:Bucket/${Id}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Lightsail

Amazon Lightsail définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour Amazon Location

Amazon Location (préfixe de service : `geo`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Location
- Types de ressources définies par Amazon Location
- Clés de condition pour Amazon Location

Actions définies par Amazon Location

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateTrackerConsumer	Accorde l'autorisation de créer une association entre une collection de périmètres virtuels et une ressource de suivi.	Écriture	tracker*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDeleteDevicePositionHistory	Accorde l'autorisation de supprimer un lot d'historiques de position de périphérique à partir d'une ressource de suivi	Écriture	tracker*		
				geo:DeviceIds	
BatchDeleteGeofence	Autorise la suppression d'un lot de périmètres virtuels d'une collection de périmètres virtuels.	Écriture	geofence-collection*		
				geo:GeofenceIds	
BatchEvaluateGeofences	Autorise l'évaluation des positions des dispositifs par rapport à la position des périmètres virtuels dans une collection de périmètres virtuels donnée.	Écriture	geofence-collection*		
BatchGetDevicePosition	Accorde l'autorisation d'envoyer une demande par lots pour récupérer les positions de l'appareil.	Lecture	tracker*		
				geo:DeviceIds	
BatchPutGeofence	Accorde l'autorisation d'envoyer une demande par lots pour l'ajout de périmètres virtuels dans une collection de périmètres virtuels.	Écriture	geofence-collection*		
				geo:GeofenceIds	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdateDevicePosition	Accorde l'autorisation de télécharger une mise à jour de position pour un ou plusieurs appareils vers une ressource de suivi.	Écriture	tracker*		
				geo:DeviceIds	
CalculateRoute	Accorde l'autorisation de calculer des itinéraires à l'aide d'une ressource de calculateur d'itinéraires donnée	Lecture	route-calculator*		
CalculateRouteMatrix	Accorde l'autorisation de calculer une matrice d'itinéraire à l'aide d'une ressource de calculateur d'itinéraires donnée	Lecture	route-calculator*		
CreateGeofenceCollection	Accorde l'autorisation de créer une collection de périmètres virtuels.	Écrire	geofence-collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKey	Octroie l'autorisation de créer une ressource de clé d'API	Écrire	api-key*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMap	Accorde l'autorisation de créer une ressource cartographique.	Écriture	map*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlaceIndex	Accorde l'autorisation de créer une ressource d'index de lieu.	Écriture	place-index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouteCalculator	Accorde l'autorisation de créer une ressource de calculateur d'itinéraires	Écriture	route-calculator*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTracker	Accorde l'autorisation de créer une ressource de suivi.	Écriture	tracker*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGeofenceCollection	Accorde l'autorisation de supprimer une collection de périmètres virtuels	Écrire	geofence-collection*		
DeleteKey	Octroie l'autorisation de supprimer une ressource de clé d'API	Écrire	api-key*		
DeleteMap	Accorde l'autorisation de supprimer une ressource cartographique.	Écriture	map*		
DeletePlaceIndex	Accorde l'autorisation de supprimer une ressource d'index de lieu.	Écriture	place-index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRouteCalculator	Accorde l'autorisation de supprimer une ressource de calculateur d'itinéraires	Écriture	route-calculator*		
DeleteTracker	Accorde l'autorisation de supprimer une ressource de suivi.	Écriture	tracker*		
DescribeGeofenceCollection	Accorde l'autorisation de récupérer les informations d'une collection de périmètres virtuels	Lecture	geofence-collection*		
DescribeKey	Octroie l'autorisation de récupérer les informations et le secret d'une ressource de clé d'API	Lecture	api-key*		
DescribeMap	Accorde l'autorisation de récupérer les informations d'une ressource cartographique	Lecture	map*		
DescribePlaceIndex	Accorde l'autorisation de récupérer les informations d'une ressource d'index de lieu	Lecture	place-index*		
DescribeRouteCalculator	Accorde l'autorisation de récupérer les détails des ressources du calculateur d'itinéraires	Lecture	route-calculator*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTracker	Accorde l'autorisation de récupérer des informations d'une ressource de suivi.	Lecture	tracker*		
DisassociateTrackerConsumer	Accorde l'autorisation de supprimer l'association entre une ressource de suivi et une collection de périmètres virtuels.	Écrire	tracker*		
ForecastGeofenceEvents	Autorise la prévision des événements pour les géofences stockées dans une collection de géofences donnée	Lecture	geofence-collection*		
GetDevicePosition	Accorde l'autorisation de récupérer la position la plus récente de l'appareil.	Lecture	tracker*		
				geo:DeviceIds	
GetDevicePositionHistory	Accorde l'autorisation de récupérer l'historique de position de l'appareil	Lecture	tracker*		
				geo:DeviceIds	
GetGeofence	Accorde l'autorisation de récupérer des détails de périmètre virtuel à partir d'une collection de périmètres virtuels	Lecture	geofence-collection*		
				geo:GeofenceIds	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMapGlyphs	Accorde l'autorisation de récupérer le fichier glyphe pour une ressource cartographique.	Lecture	map*		
GetMapSprites	Accorde l'autorisation de récupérer le fichier sprite pour une ressource cartographique.	Lecture	map*		
GetMapStyleDescriptor	Accorde l'autorisation de récupérer le descripteur de style de carte à partir d'une ressource cartographique.	Lecture	map*		
GetMapTile	Accorde l'autorisation de récupérer la vignette de carte à partir de la ressource cartographique.	Lecture	map*		
GetPlace	Accorde l'autorisation de rechercher un lieu par son ID unique	Lecture	place-index*		
ListDevicePositions	Accorde l'autorisation de récupérer une liste d'appareils et leurs dernières positions à partir de la ressource de suivi donnée	Lecture	tracker*		
ListGeofenceCollections	Accorde l'autorisation de répertorier des collections de périmètres virtuels.	Liste	geofence-collection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGeofences	Accorde l'autorisation de répertorier des périmètres virtuels stockés dans une collection donnée de périmètres virtuels.	Lecture	geofence-collection*		
ListKeys	Octroie l'autorisation de répertorier des ressources de clé d'API	List	api-key*		
ListMaps	Accorde l'autorisation de répertorier des ressources cartographiques.	Liste	map*		
ListPlaceIndexes	Accorde l'autorisation de renvoyer une liste de ressources d'index de lieu.	Liste	place-index*		
ListRouteCalculators	Accorde l'autorisation de renvoyer une liste de ressources de calculateur d'itinéraires	Liste	route-calculator*		
ListTagsForResource	Accorde l'autorisation de récupérer les identifications (métadonnées) que vous avez affectées à la ressource	Lecture	api-key		
			geofence-collection		
			map		
			place-index		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			route-calculator		
			tracker		
ListTrackerConsumers	Accorde l'autorisation de récupérer une liste de collections de périmètres virtuels actuellement associées à la ressource de suivi donnée.	Lecture	tracker*		
ListTrackers	Accorde l'autorisation de renvoyer une liste de ressources de suivi.	Liste	tracker*		
PutGeofence	Accorde l'autorisation d'ajouter un nouveau périmètre virtuel ou la mise à jour d'un périmètre virtuel existant au niveau d'une collection donnée de périmètres virtuels.	Écriture	geofence-collection*		
				geo:GeofenceIds	
SearchPlaceIndexForPosition	Accorde l'autorisation d'inverser des géocodes d'une coordonnée donnée.	Lecture	place-index*		
SearchPlaceIndexForSuggestions	Accorde l'autorisation de générer des suggestions d'adresses et de points d'intérêt basés sur du texte libre partiel ou mal orthographié	Lecture	place-index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchPlaceIndexForText	Accorde l'autorisation de géocoder du texte libre, notamment une adresse, un nom, une ville ou une région.	Lecture	place-index*		
TagResource	Accorde l'autorisation d'ajouter ou de modifier les identifications de la ressource spécifiée Les identifications sont des métadonnées qui peuvent être utilisées pour gérer une ressource.	Balisage	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les identifications données (métadonnées) de la ressource	Identification	api-key		
			geofence-collection		
			map		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			place-index		
			route-calculator		
			tracker		
				aws:TagKeys	
UpdateGeofenceCollection	Accorde l'autorisation de mettre à jour une collection de périmètres virtuels	Écrire	geofence-collection*		
UpdateKey	Octroie l'autorisation de mettre à jour une ressource de clé d'API	Écrire	api-key*		
UpdateMap	Accorde l'autorisation de mettre à jour une ressource cartographique	Écrire	map*		
UpdatePlaceIndex	Accorde l'autorisation de mettre à jour une ressource d'index de lieu	Écrire	place-index*		
UpdateRouteCalculator	Accorde l'autorisation de mettre à jour une ressource de calculateur d'acheminements	Écrire	route-calculator*		
UpdateTracker	Accorde l'autorisation de créer une ressource de suivi	Écrire	tracker*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
VerifyDevicePosition	Accorde l'autorisation de vérifier la position d'un appareil	Lecture	tracker*		
				geo:DeviceIds	

Types de ressources définies par Amazon Location

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
api-key	`arn:${Partition}:geo:${Region}:${Account}:api-key/${KeyName}`	aws:ResourceTag/${TagKey}
geofence-collection	`arn:${Partition}:geo:${Region}:${Account}:geofence-collection/${GeofenceCollectionName}`	aws:ResourceTag/${TagKey} geo:GeofenceIds
map	`arn:${Partition}:geo:${Region}:${Account}:map/${MapName}`	aws:ResourceTag/${TagKey}
place-index	`arn:${Partition}:geo:${Region}:${Account}:place-index/${IndexName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
route-calculator	`arn:${Partition}:geo:${Region}:${Account}:route-calculator/${CalculatorName}`	aws:ResourceTag/${TagKey}
tracker	`arn:${Partition}:geo:${Region}:${Account}:tracker/${TrackerName}`	aws:ResourceTag/${TagKey} geo:DeviceIds

Clés de condition pour Amazon Location

Amazon Location définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString
geo:DeviceIds	Filtre l'accès en fonction de la présence d'ID dans la demande	ArrayOfString

Clés de condition	Description	Type
geo:GeofenceIds	Filtre l'accès en fonction de la présence d'ID de périmètre virtuel dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les cartes Amazon Location Service

Amazon Location Service Maps (préfixe de service :`geo-maps`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Location Service Maps
- Types de ressources définis par Amazon Location Service Maps
- Clés de condition pour les cartes Amazon Location Service

Actions définies par Amazon Location Service Maps

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStaticMap	Accorde l'autorisation de récupérer la carte statique	Lecture	provider*		
GetTile	Accorde l'autorisation de récupérer la vignette de la carte	Lecture	provider*		

Types de ressources définis par Amazon Location Service Maps

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
provider	`arn:${Partition}:geo-maps:${Region}::provider/default`	

Clés de condition pour les cartes Amazon Location Service

Geo Maps ne possède aucune clé de contexte spécifique à un service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Location Service Places

Amazon Location Service Places (préfixe de service :`geo-places`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Location Service Places
- Types de ressources définis par Amazon Location Service Places
- Clés de condition pour Amazon Location Service Places

Actions définies par Amazon Location Service Places

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Autocomplete	Accorde l'autorisation de saisie automatique de texte avec des lieux et adresses potentiels au fur et à mesure que l'utilisateur tape	Lecture	provider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Geocode	Autorise le géocodage d'une adresse textuelle ou d'un lieu en coordonnées géographiques	Lecture	provider*		
GetPlace	Accorde l'autorisation d'interroger un lieu à l'aide de son identifiant de lieu unique	Lecture	provider*		
ReverseGeocode	Autorise la conversion des coordonnées géographiques en une adresse ou un lieu lisible par l'homme	Lecture	provider*		
SearchNearby	Permet de récupérer des lieux situés à proximité d'une position qui correspondent à un ensemble de restrictions définies par l'utilisateur, telles que la catégorie ou le type de nourriture proposé par le lieu	Lecture	provider*		
SearchText	Permet de rechercher des lieux à l'aide d'une seule saisie de texte libre	Lecture	provider*		
Suggest	Accorde l'autorisation de suggérer des lieux potentiels en fonction des informations saisies par l'utilisateur	Lecture	provider*		

Types de ressources définis par Amazon Location Service Places

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
provider	`arn:${Partition}:geo-places:${Region}::provider/default`	

Clés de condition pour Amazon Location Service Places

Geo Places ne possède aucune clé de contexte spécifique à un service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Location Service Routes

Amazon Location Service Routes (préfixe de service :`geo-routes`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Location Service Routes

- Types de ressources définis par Amazon Location Service Routes
- Clés de condition pour les itinéraires d'Amazon Location Service

Actions définies par Amazon Location Service Routes

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CalculateIsolines	Octroie l'autorisation de déterminer les destinations ou les zones de service accessibles dans un délai spécifié	Lecture	provider*		
CalculateRouteMatrix	Autorise le calcul d'une matrice de routage fournissant le temps de trajet et les distances entre des ensembles d'origines et de destinations	Lecture	provider*		
CalculateRoutes	Autorise le calcul des itinéraires entre deux emplacements ou plus	Lecture	provider*		
OptimizeWaypoints	Permet de calculer la séquence la plus efficace pour visiter plusieurs points ou lieux le long d'un itinéraire	Lecture	provider*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SnapToRoads	Permet d'améliorer la précision du positionnement géographique en alignant les coordonnées GPS sur les segments de route les plus proches sur une carte numérique	Lecture	provider*		

Types de ressources définis par Amazon Location Service Routes

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
provider	`arn:${Partition}:geo-routes:${Region}::provider/default`	

Clés de condition pour les itinéraires d'Amazon Location Service

Geo Routes ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Lookout for Equipment

Amazon Lookout for Equipment (préfixe de service : `lookoutequipment`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Lookout for Equipment
- Types de ressources définies par Amazon Lookout for Equipment
- Clés de condition pour Amazon Lookout for Equipment

Actions définies par Amazon Lookout for Equipment

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataset	Accorde l'autorisation de créer un jeu de données.	Écriture	dataset*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateInferenceScheduler	Accorde l'autorisation de créer un planificateur d'inférence pour un modèle entraîné	Écrire	inference-scheduler*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabel	Accorde l'autorisation de créer une étiquette	Écrire	label-group*		
CreateLabelGroup	Accorde l'autorisation de créer une étiquette de groupe	Écrire	label-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Accorde l'autorisation de créer un modèle entraîné sur un jeu de données	Écrire	dataset*		
			model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetrainingScheduler	Accorde l'autorisation de créer un planificateur de réentraînement pour un modèle entraîné	Écrire	model*		
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données.	Écriture	dataset*		
DeleteInferenceScheduler	Accorde l'autorisation de supprimer un planificateur d'inférence	Écrire	inference-scheduler*		
DeleteLabel	Accorde l'autorisation de supprimer une étiquette	Écrire	label-group*		
DeleteLabelGroup	Accorde l'autorisation de supprimer une étiquette de groupe	Écrire	label-group*		
DeleteModel	Accorde l'autorisation de supprimer un modèle	Écrire	model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource	Écrire	dataset		
			model		
			model-version		
DeleteRetrainingScheduler	Accorde l'autorisation de supprimer un planificateur de réentraînement d'un modèle entraîné	Écrire	model*		
DescribeDataIngestionJob	Accorde l'autorisation de décrire une tâche d'ingestion de données	Lecture			
DescribeDataset	Accorde l'autorisation de décrire un jeu de données.	Lecture	dataset*		
DescribeInferenceScheduler	Accorde l'autorisation de décrire un planificateur d'inférence	Lecture	inference-scheduler*		
DescribeLabelGroup	Accorde l'autorisation de décrire une étiquette de groupe	Lecture	label-group*		
DescribeModel	Accorde l'autorisation de décrire un modèle	Lecture	model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeModelVersion	Octroie l'autorisation de décrire une version de modèle.	Lecture	model-version*		
DescribeResourcePolicy	Octroie l'autorisation de décrire une stratégie de ressources.	Lecture	dataset		
			model		
			model-version		
DescribeRetrainingScheduler	Accorde l'autorisation de décrire un planificateur de réentraînement d'un modèle entraîné	Lecture	model*		
DescribeLabel	Accorde l'autorisation de décrire une étiquette	Lecture	label-group*		
ImportDataset	Octroie l'autorisation d'importer un jeu de données.	Écrire	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ImportModelVersion	Octroie l'autorisation d'importer une version de modèle.	Écrire	dataset*		
			model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys lookoutequipment:IsImportingData	
ListDataIngestionJobs	Accorde l'autorisation de répertorier les tâches d'ingestion de données dans votre compte ou pour un jeu de données particulier	Liste	dataset*		
ListDatasets	Accorde l'autorisation de répertorier les jeux de données de votre compte	List			
ListInferenceEvents	Accorde l'autorisation de répertorier les évènements d'inférence pour un planificateur d'inférence	Lecture	inference-scheduler*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListInferenceExecutions	Accorde l'autorisation de répertorier les exécutions d'inférence pour un planificateur d'inférence	Lecture	inference-scheduler*		
ListInferenceSchedulers	Accorde l'autorisation de répertorier les planificateurs d'inférence de votre compte	List			
ListLabelGroups	Accorde l'autorisation de répertorier les groupes d'étiquettes dans votre compte	List	label-group*		
ListLabels	Accorde l'autorisation de répertorier les étiquettes dans votre compte	List	label-group*		
ListModelVersions	Octroie l'autorisation de répertorier les versions de modèles de votre compte.	List	model*		
ListModels	Accorde l'autorisation de répertorier les modèles de votre compte	List			
ListRetrainingSchedulers	Accorde l'autorisation de répertorier les planificateurs de réentraînement de votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSensorStatistics	Accorde l'autorisation de répertorier les statistiques de capteurs pour un jeu de données ou une tâche d'ingestion particulier	List	dataset*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		
PutResourcePolicy	Octroie l'autorisation de saisir une stratégie de ressources.	Écrire	dataset		
			model		
			model-version		
StartDataIngestionJob	Accorde l'autorisation de démarrer une tâche d'ingestion de données pour un jeu de données	Écriture	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartInferenceScheduler	Accorde l'autorisation de démarrer un planificateur d'inférence	Écrire	inference-scheduler*		
StartRetrainingScheduler	Accorde l'autorisation de démarrer un planificateur de réentraînement d'un modèle entraîné	Écrire	model*		
StopInferenceScheduler	Accorde l'autorisation d'arrêter un planificateur d'inférence	Écrire	inference-scheduler*		
StopRetrainingScheduler	Accorde l'autorisation d'arrêter un planificateur de réentraînement d'un modèle entraîné	Écrire	model*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		
				aws:TagKeys	
UpdateActiveModelVersion	Octroie l'autorisation de définir la version active du modèle pour un modèle de machine learning donné.	Écrire	model*		
			model-version*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateInferenceScheduler	Accorde l'autorisation de mettre à jour un planificateur d'inférence	Écrire	inference-scheduler*		
UpdateLabelGroup	Accorde l'autorisation de mettre à jour une étiquette de groupe	Écrire	label-group*		
UpdateModel	Accorde l'autorisation de mettre à jour un modèle entraîné	Écrire	model*		
UpdateRetrainingScheduler	Accorde l'autorisation de mettre à jour un planificateur de réentraînement d'un modèle entraîné	Écrire	model*		

Types de ressources définies par Amazon Lookout for Equipment

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
dataset	`arn:${Partition}:lookoutequipment:${Region}:${Account}:dataset/${DatasetName}/${DatasetId}`	aws:ResourceTag/${TagKey}
model	`arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}`	aws:ResourceTag/${TagKey}
model-version	`arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}/model-version/${ModelVersionNumber}`	aws:ResourceTag/${TagKey}
inference-scheduler	`arn:${Partition}:lookoutequipment:${Region}:${Account}:inference-scheduler/${InferenceSchedulerName}/${InferenceSchedulerId}`	aws:ResourceTag/${TagKey}
label-group	`arn:${Partition}:lookoutequipment:${Region}:${Account}:label-group/${LabelGroupName}/${LabelGroupId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Lookout for Equipment

Amazon Lookout for Equipment définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
lookoutequipment:IsImportingData	Filtre l'accès en fonction de la stratégie d'importation des données sous-jacentes	Booléen

Actions, ressources et clés de condition pour Amazon Lookout for Metrics

Amazon Lookout for Metrics (préfixe de service : `lookoutmetrics`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Lookout for Metrics
- Types de ressources définies par Amazon Lookout for Metrics
- Clés de condition pour Amazon Lookout for Metrics

Actions définies par Amazon Lookout for Metrics

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateAnomalyDetector	Accorde l'autorisation d'activer un détecteur d'anomalies	Écriture	AnomalyDetector*		
BackTestAnomalyDetector	Accorde l'autorisation d'exécution d'un rétro-test avec un détecteur d'anomalies	Écriture	AnomalyDetector*		
CreateAlert	Accorde l'autorisation de créer une alerte pour un détecteur d'anomalies	Écriture	Alert*		
			AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalyDetector	Accorde l'autorisation de créer un détecteur d'anomalies	Écriture	AnomalyDetector*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateMetricSet	Accorde l'autorisation de créer un jeu de données.	Écrire	AnomalyDetector*		
			MetricSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateAnomalyDetector	Accorde l'autorisation de désactiver un détecteur d'anomalies	Écrire	AnomalyDetector*		
DeleteAlert	Accorde l'autorisation de supprimer une alerte.	Écriture	Alert*		
DeleteAnomalyDetector	Accorde l'autorisation de supprimer un détecteur d'anomalies	Écriture	AnomalyDetector*		
DescribeAlert	Accorde l'autorisation d'obtenir des détails sur une alerte	Lecture	Alert*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAnomalyDetectionExecutions	Accorde l'autorisation d'obtenir des informations sur une tâche de détection d'anomalie	Lecture	AnomalyDetector*		
DescribeAnomalyDetector	Accorde l'autorisation d'obtenir des détails sur un détecteur d'anomalies	Lecture	AnomalyDetector*		
DescribeMetricSet	Accorde l'autorisation d'obtenir des détails sur un jeu de données.	Lecture	MetricSet*		
DetectMetricSetConfig	Accorde l'autorisation de détecter la configuration du jeu de métrique à partir de la source de données	Écrire	AnomalyDetector*		
GetAnomalyGroup	Accorde l'autorisation d'obtenir des détails sur un groupe de métriques affectées	Lecture	AnomalyDetector*		
GetDataQualityMetrics	Accorde l'autorisation d'obtenir des métriques de qualité des données pour un détecteur d'anomalies	Lecture	AnomalyDetector*		
GetFeedback	Accorde l'autorisation d'obtenir des commentaires sur les métriques affectées pour un groupe d'anomalies	Lecture	AnomalyDetector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSampleData	Accorde l'autorisation d'obtenir une sélection d'exemples d'enregistrements à partir d'une source de données Amazon S3	Lecture			
ListAlerts	Accorde l'autorisation d'obtenir une liste d'alertes pour un détecteur	Liste	AnomalyDetector		
ListAnomalyDetectors	Accorde l'autorisation d'obtenir une liste de détecteurs d'anomalies	List			
ListAnomalyGroupRelatedMetrics	Accorde l'autorisation d'obtenir une liste des mesures liées dans un groupe d'anomalies	List	AnomalyDetector*		
ListAnomalyGroupSummaries	Accorde l'autorisation d'obtenir une liste de groupes d'anomalies	Liste	AnomalyDetector*		
ListAnomalyGroupTimeSeries	Accorde l'autorisation d'obtenir une liste des métriques affectées pour une mesure dans un groupe d'anomalies	Liste	AnomalyDetector*		
ListMetricSets	Accorde l'autorisation d'obtenir une liste de jeux de données	Liste	AnomalyDetector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation d'obtenir une liste de balises pour un détecteur, un jeu de données ou une alerte	Lecture	Alert		
			AnomalyDetector		
			MetricSet		
PutFeedback	Accorde l'autorisation d'ajouter des commentaires pour une métrique affectée dans un groupe d'anomalies	Écriture	AnomalyDetector*		
TagResource	Accorde l'autorisation d'ajouter des balises à un détecteur, à un jeu de données ou à une alerte	Balisage	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des balises d'un détecteur, d'un jeu de données ou d'une alerte	Identification	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys	
UpdateAlert	Accorde l'autorisation de mettre à jour une alerte pour un détecteur d'anomalies	Écrire	Alert*		
UpdateAnomalyDetector	Accorde l'autorisation de mettre à jour un détecteur d'anomalies	Écriture	AnomalyDetector*		
UpdateMetricSet	Accorde l'autorisation de mettre à jour un jeu de données.	Écriture	MetricSet*		

Types de ressources définies par Amazon Lookout for Metrics

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AnomalyDetector	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:AnomalyDetector:${AnomalyDetectorName}`	aws:ResourceTag/${TagKey}
MetricSet	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:MetricSet/${AnomalyDetectorName}/${MetricSetName}`	aws:ResourceTag/${TagKey}
Alert	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:Alert:${AlertName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Lookout for Metrics

Amazon Lookout for Metrics définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Lookout for Vision

Amazon Lookout for Vision (préfixe de service : `lookoutvision`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Lookout for Vision
- Types de ressources définies par Amazon Lookout for Vision
- Clés de condition pour Amazon Lookout for Vision

Actions définies par Amazon Lookout for Vision

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataset	Accorde l'autorisation de créer un manifeste de jeu de données.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateModel	Accorde l'autorisation de créer un nouveau modèle de détection d'anomalies.	Écriture	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Accorde l'autorisation de créer un projet.	Écriture	project*		
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données.	Écriture			
DeleteModel	Accorde l'autorisation de supprimer un modèle et toutes les ressources associées.	Écriture	model*		
DeleteProject	Accorde l'autorisation de supprimer un projet de manière irréversible.	Écriture	project*		
DescribeDataset	Accorde l'autorisation d'afficher des informations détaillées sur le manifeste de jeu de données.	Lecture			
DescribeModel	Accorde l'autorisation d'afficher des informations détaillées sur un modèle.	Lecture	model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeModelPackagingJob	Accorde l'autorisation d'afficher des informations détaillées sur une tâche d'empaquetage de modèle	Lecture			
DescribeProject	Accorde l'autorisation d'afficher des informations détaillées sur un projet.	Lecture	project*		
DescribeTrialDetection [autorisation uniquement]	Accorde l'autorisation de fournir des informations d'état sur une tâche de détection d'anomalie en cours d'exécution.	Lecture			
DetectAnomalies	Accorde l'autorisation d'invoquer la détection d'anomalies.	Écriture	model*		
ListDatasetEntries	Accorde l'autorisation de répertorier les contenus du manifeste de jeu de données.	Lecture			
ListModelPackagingJobs	Accorde l'autorisation de répertorier toutes les tâches d'empaquetage de modèles associées à un projet	List			
ListModels	Accorde l'autorisation de répertorier tous les modèles associés à un projet.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProjects	Accorde l'autorisation de répertorier tous les projets.	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	model		
ListTrialDetections [autorisation uniquement]	Accorde l'autorisation de répertorier toutes les tâches de détection d'anomalies.	Liste			
StartModel	Accorde l'autorisation de démarrer le modèle de détection d'anomalies.	Écrire	model*		
StartModelPackagingJob	Accorde l'autorisation de démarrer une tâche d'empaquetage de modèle	Écrire	model*		
StartTrialDetection [autorisation uniquement]	Accorde l'autorisation de lancer la détection en bloc d'anomalies pour un jeu d'images stockées dans un compartiment S3.	Écriture			
StopModel	Accorde l'autorisation d'arrêter le modèle de détection d'anomalies.	Écrire	model*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Identification	model		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer la balise avec la clé donnée d'une ressource	Identification	model		
				aws:TagKeys	
UpdateDatasetEntries	Accorde l'autorisation de mettre à jour un manifeste de jeu de données d'entraînement ou de test.	Écriture			

Types de ressources définies par Amazon Lookout for Vision

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
model	arn:${Partition}:lookoutvision:${Region}:${Account}:model/${ProjectName}/${ModelVersion}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:lookoutvision:${Region}:${Account}:project/${ProjectName}	

Clés de condition pour Amazon Lookout for Vision

Amazon Lookout for Vision définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Machine Learning

Amazon Machine Learning (préfixe de service : `machinelearning`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Machine Learning
- Types de ressources définis par Amazon Machine Learning
- Clés de condition pour Amazon Machine Learning

Actions définies par Amazon Machine Learning

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTags	Ajoute une ou plusieurs balises à un objet, dans la limite de 10. Chaque balise est constituée d'une clé et d'une valeur facultative	Balisage	batchprediction		
			datasource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			evaluation		
			mlmodel		
CreateBatchPrediction	Génère des prédictions pour un groupe d'observations.	Écrire	batchprediction*		
			datasource*		
			mlmodel*		
CreateDataSourceFromRDS	Crée un DataSource objet à partir d'un Amazon RDS	Écrire	datasource*		
CreateDataSourceFromRedshift	Crée un DataSource à partir d'une base de données hébergée sur un cluster Amazon Redshift	Écrire	datasource*		
CreateDataSourceFromS3	Crée un DataSource objet à partir de S3	Écrire	datasource*		
CreateEvaluation	Crée une nouvelle évaluation d'un MLModel	Écrire	datasource*		
			evaluation*		
			mlmodel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMLModel	Crée un nouveau MLModel	Écrire	datasource*		
			mlmodel*		
CreateRealtimeEndpoint	Crée un point de terminaison en temps réel pour MLModel	Écrire	mlmodel*		
DeleteBatchPrediction	Attribue le statut DELETED à un BatchPrediction, le rendant inutilisable	Écrire	batchprediction*		
DeleteDataSource	Attribue le statut DELETED à un DataSource, le rendant inutilisable	Écrire	datasource*		
DeleteEvaluation	Attribue le statut DELETED à un objet Evaluation, cela le rendant inutilisable.	Écrire	evaluation*		
DeleteMLModel	Attribue le statut DELETED à un MLModel, le rendant inutilisable	Écrire	mlmodel*		
DeleteRealtimeEndpoint	Supprime un point de terminaison en temps réel d'un MLModel	Écrire	mlmodel*		
DeleteTags	Supprime les balises spécifiées associés à un objet ML. Une fois cette opération terminée, vous ne pouvez pas récupérer les balises supprimées.	Identification	batchprediction		
			datasource		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			evaluation		
			mlmodel		
DescribeBatchPredictions	Renvoie une liste des BatchPrediction opérations qui correspondent aux critères de recherche de la demande	List			
DescribeDataSources	Renvoie une liste de ceux DataSource qui correspondent aux critères de recherche de la demande	List			
DescribeEvaluations	Renvoie une liste de ceux DescribeEvaluations qui correspondent aux critères de recherche de la demande	List			
DescribeMLModels	Renvoie une liste de ceux MLModel qui correspondent aux critères de recherche de la demande	List			
DescribeTags	Décrit une ou plusieurs des balises de votre objet Amazon ML.	List	batchprediction		
			datasource		
			evaluation		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			mlmodel		
GetBatchPrediction	Renvoie un BatchPrediction qui inclut des informations détaillées sur les métadonnées, le statut et les fichiers de données	Lecture	batchprediction*		
GetDataSource	Renvoie un DataSource qui inclut les métadonnées et les informations du fichier de données, ainsi que l'état actuel du DataSource	Lecture	datasource*		
GetEvaluation	Renvoie un objet Evaluation qui inclut les métadonnées, ainsi que le statut actuel de l'objet Evaluation.	Lecture	datasource*		
GetMLModel	Renvoie un MLModel qui inclut des métadonnées détaillées et des informations sur la source de données, ainsi que l'état actuel du MLModel	Lecture	mlmodel*		
Predict	Génère une prédiction pour l'observation à l'aide du modèle ML spécifié.	Écrire	mlmodel*		
UpdateBatchPrediction	Met BatchPredictionName à jour le BatchPrediction	Écrire	batchprediction*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataSource	Met DataSourceName à jour le DataSource	Écrire	datasource*		
UpdateEvaluation	Met à jour le EvaluationName contenu d'une évaluation	Écrire	evaluation*		
UpdateMLModel	Met à jour le MLModel nom et le nom ScoreThreshold d'un MLModel	Écrire	mlmodel*		

Types de ressources définis par Amazon Machine Learning

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
batchprediction	`arn:${Partition}:machinelearning:${Region}:${Account}:batchprediction/${BatchPredictionId}`	
datasource	`arn:${Partition}:machinelearning:${Region}:${Account}:datasource/${DatasourceId}`	

Types de ressources	ARN	Clés de condition
evaluation	`arn:${Partition}:machinelearning:${Region}:${Account}:evaluation/${EvaluationId}`	
mlmodel	`arn:${Partition}:machinelearning:${Region}:${Account}:mlmodel/${MlModelId}`	

Clés de condition pour Amazon Machine Learning

Machine Learning ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Macie

Amazon Macie (préfixe de service : `macie2`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Macie
- Types de ressources définis par Amazon Macie
- Clés de condition pour Amazon Macie

Actions définies par Amazon Macie

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> Les GetMasterAccount actions DisassociateFromMasterAccount et sont devenues obsolètes. Nous vous recommandons de spécifier les GetAdministratorAccount actions DisassociateFromAdministratorAccount et respectivement à la place.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptInvitation	Accorde l'autorisation d'accepter une invitation d'adhésion à Amazon Macie	Écriture			
BatchGetCustomDataIdentifiers	Accorde l'autorisation de récupérer des informations sur un ou plusieurs identificateurs de données personnalisés	Lecture	CustomDataIdentifier*		
BatchUpdateAutomatedDiscoveryAccounts	Autorise un administrateur Amazon Macie à modifier le statut de la découverte automatique des données sensibles pour un ou plusieurs comptes de son organisation	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAllowList	Accorde l'autorisation de créer et de définir les paramètres d'une liste d'autorisation	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateClassificationJob	Accorde l'autorisation de créer et de définir les paramètres d'une tâche de découverte de données sensibles	Écriture	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDataIdentifier	Accorde l'autorisation de créer et de définir les paramètres d'un identificateur de données personnalisé	Écriture	CustomDataIdentifier*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsFilter	Accorde l'autorisation de créer et de définir les paramètres d'un filtre de résultats	Écriture	FindingsFilter*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvitations	Accorde l'autorisation d'envoyer une invitation d'adhésion à Amazon Macie	Écriture			
CreateMember	Accorde l'autorisation d'associer un compte à un compte administrateur Amazon Macie	Écriture	Member*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSampleFindings	Accorde l'autorisation de créer des exemples de résultats.	Écriture			
DeclineInvitations	Accorde l'autorisation de refuser les invitations d'adhésion à Amazon Macie	Écrire			
DeleteAllowList	Accorde l'autorisation de supprimer une liste d'autorisation	Écrire	AllowList*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCustomDataIdentifier	Accorde l'autorisation de supprimer un identificateur de données personnalisé	Écriture	CustomDataIdentifier*		
DeleteFindingsFilter	Accorde l'autorisation de supprimer un filtre de résultats	Écriture	FindingsFilter*		
DeleteInvitations	Accorde l'autorisation de supprimer les invitations d'adhésion à Amazon Macie	Écriture			
DeleteMember	Accorde l'autorisation de supprimer l'association entre un compte administrateur Amazon Macie et un compte	Écriture	Member*		
DescribeBuckets	Accorde l'autorisation de récupérer des données statistiques et autres sur les compartiments S3 qu'Amazon Macie surveille et analyse	Lecture			
DescribeClassificationJob	Accorde l'autorisation de récupérer des informations sur l'état et les paramètres d'une tâche de découverte de données sensibles	Lecture	ClassificationJob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeOrganizationConfiguration	Accorde l'autorisation de récupérer des informations sur les paramètres de configuration d'Amazon Macie pour une organisation AWS	Lecture			
DisableMacie	Accorde l'autorisation de désactiver un compte Amazon Macie, ce qui supprime également les ressources Macie pour le compte	Écrire			
DisableOrganizationAdminAccount	Accorde l'autorisation de désactiver un compte en tant que compte administrateur Amazon Macie délégué pour une organisation AWS	Écrire			
DisassociateFromAdministratorAccount	Accorde l'autorisation à un compte membre Amazon Macie de se dissocier de son compte administrateur Macie	Écrire			
DisassociateFromMasterAccount	Accorde l'autorisation à un compte membre Amazon Macie de se dissocier de son compte administrateur Macie	Écrire			
DisassociateMember	Accorde l'autorisation à un compte administrateur Amazon Macie de se dissocier d'un compte membre Macie	Écrire	Member*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableMacie	Accorde l'autorisation d'activer et de spécifier les paramètres de configuration d'un nouveau compte Amazon Macie	Écrire			
EnableOrganizationAdminAccount	Accorde l'autorisation d'activer un compte en tant que compte administrateur Amazon Macie délégué pour une organisation AWS	Écrire			
GetAdministratorAccount	Accorde l'autorisation de récupérer des informations sur le compte administrateur Amazon Macie pour un compte	Lecture			
GetAllowList	Accorde l'autorisation de récupérer les paramètres et l'état d'une liste d'autorisation	Lecture	AllowList*		
GetAutomatedDiscoveryConfiguration	Accorde l'autorisation de récupérer les paramètres de configuration et l'état de la découverte automatique des données sensibles pour un compte administrateur, une organisation ou un compte autonome Amazon Macie	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBucketStatistics	Accorde l'autorisation de récupérer des données statistiques agrégées pour tous les compartiments S3 qu'Amazon Macie surveille et analyse	Lecture			
GetClassificationExportConfiguration	Accorde l'autorisation de récupérer les paramètres d'exportation des résultats de découverte de données sensibles	Lecture			
GetClassificationScope	Accorde l'autorisation de récupérer les paramètres de la portée de la classification pour un compte	Lecture			
GetCustomDataIdentifier	Accorde l'autorisation de récupérer des informations sur les paramètres d'un identificateur de données personnalisé	Lecture	CustomDataIdentifier*		
GetFindingStatistics	Accorde l'autorisation de récupérer des données statistiques agrégées sur les résultats	Lecture			
GetFindings	Accorde l'autorisation de récupérer les détails d'un ou plusieurs résultats	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFindingsFilter	Accorde l'autorisation de récupérer des informations sur les paramètres d'un filtre de résultats	Lecture	FindingsFilter*		
GetFindingsPublicationConfiguration	Accorde l'autorisation de récupérer les paramètres de configuration pour publier les résultats sur AWS Security Hub	Lecture			
GetInvitationsCount	Accorde l'autorisation de récupérer le nombre d'invitations d'adhésion à Amazon Macie reçues par un compte	Lecture			
GetMacieSession	Accorde l'autorisation de récupérer des informations sur l'état et les paramètres de configuration d'un compte Amazon Macie	Lecture			
GetMasterAccount	Accorde l'autorisation de récupérer des informations sur le compte administrateur Amazon Macie pour un compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMember	Accorde l'autorisation de récupérer des informations sur un compte associé à un compte administrateur Amazon Macie	Lecture	Member*		
GetResourceProfile	Accorde l'autorisation de récupérer les statistiques de découverte de données sensibles et le score de sensibilité d'un compartiment S3	Lecture			
GetRevealConfiguration	Accorde l'autorisation de récupérer le statut et les paramètres de configuration pour la récupération des occurrences de données sensibles signalées par les résultats	Lecture			
GetSensitiveDataOccurrences	Accorde l'autorisation de récupérer les occurrences de données sensibles signalées par un résultat	Lecture			
GetSensitiveDataOccurrencesAvailability	Accorde l'autorisation de vérifier si les occurrences de données sensibles peuvent être récupérées par un résultat	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSensitivityInspectionTemplate	Accorde l'autorisation de récupérer les paramètres du modèle d'inspection de la sensibilité pour un compte	Lecture			
GetUsageStatistics	Accorde l'autorisation de récupérer des quotas et des données d'utilisation agrégées pour un ou plusieurs comptes	Lecture			
GetUsageTotals	Accorde l'autorisation de récupérer des données d'utilisation agrégées pour un compte	Lecture			
ListAllowLists	Accorde l'autorisation de récupérer un sous-ensemble d'informations sur toutes les listes d'autorisation pour un compte	List			
ListAutomatedDiscoveryAccounts	Accorde l'autorisation de récupérer l'état de la découverte automatique des données sensibles pour un compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListClassificationJobs	Accorde l'autorisation de récupérer un sous-ensemble d'informations sur l'état et les paramètres d'une ou plusieurs tâches de découverte de données sensibles	List			
ListClassification Scopes	Accorde l'autorisation de récupérer un sous-ensemble d'informations sur la portée de la classification d'un compte	List			
ListCustomDataIdentifiers	Accorde l'autorisation de récupérer des informations sur tous les identificateurs de données personnalisés	Liste			
ListFindings	Accorde l'autorisation de récupérer un sous-ensemble d'informations sur un ou plusieurs résultats	Liste			
ListFindingsFilters	Accorde l'autorisation de récupérer des informations sur tous les filtres de résultats	Liste			
ListInvitations	Accorde l'autorisation de récupérer des informations sur toutes les invitations d'adhésion à Amazon Macie reçues par un compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListManagedDataIdentifiers	Accorde l'autorisation de récupérer des informations sur les identificateurs de données gérés	List			
ListMembers	Accorde l'autorisation de récupérer des informations sur les comptes membres Amazon Macie associés à un compte administrateur Amazon Macie	List			
ListOrganizationAdminAccounts	Accorde l'autorisation de récupérer des informations sur le compte administrateur Amazon Macie délégué à une organisation AWS	List			
ListResourceProfileArtifacts	Accorde l'autorisation de récupérer des informations sur les objets sélectionnés par Amazon Macie dans un compartiment S3 pour la découverte automatique de données sensibles	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceProfileDetections	Accorde l'autorisation de récupérer des informations sur les types et la quantité de données sensibles qu'Amazon Macie a trouvées dans un compartiment S3	List			
ListSensitivityInspectionTemplates	Accorde l'autorisation de récupérer un sous-ensemble d'informations sur le modèle d'inspection de la sensibilité pour un compte	List			
ListTagsForResource	Accorde l'autorisation de récupérer les balises d'une ressource Amazon Macie	Lecture	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
PutClassificationExportConfiguration	Accorde l'autorisation de créer ou de mettre à jour les paramètres de stockage des résultats de découverte de données sensibles	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutFindingsPublicationConfiguration	Autorise la mise à jour des paramètres de configuration pour la publication des résultats sur AWS Security Hub	Écrire			
SearchResources	Accorde l'autorisation de récupérer des données statistiques et d'autres informations sur AWS les ressources surveillées et analysées par Amazon Macie	Lecture			
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour les balises d'une ressource Amazon Macie	Balisage	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestCustomDataIdentifier	Accorde l'autorisation de tester un identificateur de données personnalisé	Écriture			
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource Amazon Macie.	Identification	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
				aws:TagKeys	
UpdateAllowList	Accorde l'autorisation de mettre à jour les paramètres d'une liste d'autorisation	Écrire	AllowList*		
UpdateAutomatedDiscoveryConfiguration	Accorde l'autorisation de modifier le statut de la découverte automatique des données sensibles pour un compte administrateur, une organisation ou un compte autonome Amazon Macie	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateClassificationJob	Accorde l'autorisation de modifier l'état d'une tâche de découverte de données sensibles	Écrire	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateClassificationScope	Accorde l'autorisation de mettre à jour les paramètres de la portée de la classification pour un compte	Écrire			
UpdateFindingsFilter	Accorde l'autorisation de mettre à jour les paramètres d'un filtre de résultats	Écrire	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMacieSession	Autorise un compte administrateur Amazon Macie à suspendre ou à réactiver Macie pour un compte membre	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMemberSession	Accorde l'autorisation à un compte administrateur Amazon Macie de suspendre ou de réactiver un compte membre Macie	Écrire			
UpdateOrganizationConfiguration	Accorde l'autorisation de mettre à jour les paramètres de configuration d'Amazon Macie pour une organisation AWS	Écrire			
UpdateResourceProfile	Accorde l'autorisation de mettre à jour le score de sensibilité d'un compartiment S3	Écrire			
UpdateResourceProfileDetections	Accorde l'autorisation de mettre à jour les paramètres d'évaluation de la sensibilité d'un compartiment S3	Écrire			
UpdateRevealConfiguration	Accorde l'autorisation de mettre à jour le statut et les paramètres de configuration pour la récupération des occurrences de données sensibles signalées par les résultats	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSensitivityInspectionTemplate	Accorde l'autorisation de mettre à jour les paramètres du modèle d'inspection de la sensibilité pour un compte	Écrire			

Types de ressources définis par Amazon Macie

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AllowList	`arn:${Partition}:macie2:${Region}:${Account}:allow-list/${ResourceId}`	aws:ResourceTag/${TagKey}
ClassificationJob	`arn:${Partition}:macie2:${Region}:${Account}:classification-job/${ResourceId}`	aws:ResourceTag/${TagKey}
CustomDataIdentifier	`arn:${Partition}:macie2:${Region}:${Account}:custom-data-identifier/${ResourceId}`	aws:ResourceTag/${TagKey}
FindingsFilter	`arn:${Partition}:macie2:${Region}:${Account}:findings-filter/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Member	`arn:${Partition}:macie2:${Region}:${Account}:member/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Macie

Amazon Macie définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les tests d'applications de modernisation AWS du mainframe

AWS Les tests d'applications de modernisation du mainframe (préfixe de service :`apptest`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le test des applications de modernisation du AWS mainframe
- Types de ressources définis par les tests des applications de modernisation du AWS mainframe
- Clés de condition pour les AWS tests d'applications de modernisation des ordinateurs centraux

Actions définies par le test des applications de modernisation du AWS mainframe

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTestCase	Accorde l'autorisation de créer un scénario de test	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTestConfiguration	Accorde l'autorisation de créer une configuration de test	Écrire		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateTestSuite	Accorde l'autorisation de créer une suite de tests	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTestCase	Autorise la suppression d'un scénario de test	Écrire	TestCase*		
DeleteTestConfiguration	Accorde l'autorisation de supprimer une configuration de test	Écrire	TestConfiguration*		
DeleteTestRun	Autorise la suppression d'un test	Écrire	TestRun*		s3:DeleteObject s3:ListBucket
DeleteTestSuite	Autorise la suppression d'une suite de tests	Écrire	TestSuite*		
GetTestCase	Accorde l'autorisation d'obtenir un scénario de test	Lecture	TestCase*		
GetTestConfiguration	Accorde l'autorisation d'obtenir une configuration de test	Lecture	TestConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTestRunStep	Accorde l'autorisation d'accéder à l'étape d'exécution du test	Lecture	TestRun*		
GetTestSuite	Accorde l'autorisation d'obtenir une suite de tests	Lecture	TestSuite*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture			
ListTestCases	Accorde l'autorisation de répertorier les cas de test	List			
ListTestConfigurations	Accorde l'autorisation de répertorier les configurations de test	List			
ListTestRunSteps	Octroie l'autorisation de répertorier les étapes d'un test	Lecture	TestRun*		
ListTestRunTestCases	Accorde l'autorisation de répertorier les cas de test pour une exécution de test	Lecture	TestRun*		
ListTestRuns	Accorde l'autorisation de répertorier les essais	List			
ListTestSuites	Accorde l'autorisation de répertorier les suites de tests	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartTestRun	Autorise le lancement d'un test	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:CreateStack cloudformation:DeleteStack cloudformation:DescribeStacks dms:DescribeReplicationTasks dms:StartReplicationTask dms:StopReplicationTask ec2:DescribeAvailabilityZones ec2:DescribeVpcEnd

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					pointServiceConfigurations ec2:DescribeVpcEndpointServices m2:CreateDataSetImportTask m2:GetApplication m2:GetApplicationVersion m2:GetBatchJobExecution m2:GetDataSetDetails m2:GetDataSetImportTask

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					m2:StartApplication m2:StartBatchJob m2:StopApplication s3:CreateBucket s3:DeleteObject s3:GetObject s3:ListBucket s3:PutObject
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		
				aws:TagKeys	
UpdateTestCase	Autorise la mise à jour d'un scénario de test	Écrire	TestCase*		
UpdateTestConfiguration	Accorde l'autorisation de mettre à jour une configuration de test	Écrire	TestConfiguration*		
UpdateTestSuite	Autorise la mise à jour d'une suite de tests	Écrire	TestSuite*		

Types de ressources définis par les tests des applications de modernisation du AWS mainframe

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
TestCase	`arn:${Partition}:apptest:${Region}:${Account}:testcase/${TestCaseId}`	aws:ResourceTag/${TagKey}
TestConfiguration	`arn:${Partition}:apptest:${Region}:${Account}:testconfiguration/${TestConfigurationId}`	aws:ResourceTag/${TagKey}
TestRun	`arn:${Partition}:apptest:${Region}:${Account}:testrun/${TestRunId}`	aws:ResourceTag/${TagKey}
TestSuite	`arn:${Partition}:apptest:${Region}:${Account}:testsuite/${TestSuiteId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les AWS tests d'applications de modernisation des ordinateurs centraux

AWS Les tests d'applications de modernisation du mainframe définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour le service de modernisation AWS du mainframe

AWS Le service de modernisation du mainframe (préfixe de service :m2) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service de modernisation AWS du mainframe
- Types de ressources définis par le service de modernisation AWS du mainframe
- Clés de condition pour le AWS service de modernisation des ordinateurs centraux

Actions définies par le service de modernisation AWS du mainframe

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelBatchJobExecution	Accorde l'autorisation d'annuler l'exécution d'une tâche par lot	Écrire	Application*		
CreateApplication	Accorde l'autorisation de créer une application	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateDataSetExportTask	Accorde l'autorisation de créer une tâche d'exportation d'un ensemble de données	Écrire	Application*		s3:GetObject
CreateDataSetImportTask	Accorde l'autorisation de créer une tâche d'importation de jeux de données	Écrire	Application*		s3:GetObject
CreateDeployment	Accorde l'autorisation de créer un déploiement	Écrire	Application*		elasticloadbalancing:AddTags elasticloadbalancing:CreateListener elasticloadbalanci

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ng:CreateTargetGroup elasticloadbalancing:RegisterTargets
			Environment		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEnvironment	Accorde l'autorisation de créer un environnement	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					elasticfilesystem:DescribeMountTargets elasticloadbalancing:AddTags elasticloadbalancing:CreateLoadBalancer fsx:DescribeFileSystems iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteApplicationFromEnvironment	Accorde l'autorisation de supprimer une application d'un environnement d'exécution	Écrire	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteEnvironment	Accorde l'autorisation de supprimer un environnement d'exécution	Écrire	Environment*		elasticloadbalancing:DeleteLoadBalancer
GetApplication	Accorde l'autorisation de récupérer une application	Lecture	Application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetApplicationVersion	Accorde l'autorisation de récupérer une version d'application	Lecture	Application*		
GetBatchJobExecution	Accorde l'autorisation de récupérer l'exécution d'une tâche par lot	Lecture	Application*		
GetDataSetDetails	Accorde l'autorisation de récupérer les détails d'un jeu de données	Lecture	Application*		
GetDataSetExportTask	Autorise l'exportation d'un ensemble de données à l'emplacement S3 spécifié	Lecture	Application*		
GetDataSetImportTask	Accorde l'autorisation de récupérer une tâche d'importation d'un jeu de données	Lecture	Application*		
GetDeployment	Accorde l'autorisation de récupérer un déploiement	Lecture	Application*		
GetEnvironment	Accorde l'autorisation de récupérer un environnement d'exécution	Lecture	Environment*		
GetSignedBluinsightsUrl	Octroie l'autorisation de créer une URL Bluinsights signée.	Lecture			
ListApplicationVersions	Accorde l'autorisation de lister les versions d'une application	Lecture	Application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplications	Accorde l'autorisation de répertorier les applications	List			
ListBatchJobDefinitions	Accorde l'autorisation de répertorier les définitions d'une tâche par lot	Lecture	Application*		
ListBatchJobExecutions	Accorde l'autorisation de répertorier les exécutions d'une tâche par lot	Lecture	Application*		
ListBatchJobRestartPoints	Accorde l'autorisation de récupérer l'exécution d'une tâche par lot	Lecture	Application*		
ListDataSetExportHistory	Accorde l'autorisation de répertorier l'historique des exportations d'ensembles de données	Lecture	Application*		
ListDataSetImportHistory	Accorde l'autorisation de répertorier l'historique des importations d'un jeu de données	Lecture	Application*		
ListDataSets	Accorde l'autorisation de répertorier les jeux de données	Lecture	Application*		
ListDeployments	Accorde l'autorisation de répertorier les déploiements	Lecture	Application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEngineVersions	Accorde l'autorisation de répertorier les versions d'un moteur	Lecture			
ListEnvironments	Accorde l'autorisation de répertorier les environnements d'exécution	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture			
StartApplication	Accorde l'autorisation de démarrer une application	Écrire	Application*		
StartBatchJob	Accorde l'autorisation de démarrer une tâche par lot	Écrire	Application*		
StopApplication	Accorde l'autorisation d'arrêter une application	Écrire	Application*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	Application		
			Environment		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	Application		
			Environment		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour une application	Écrire	Application*		s3:GetObject s3:ListBucket
UpdateEnvironment	Accorde l'autorisation de mettre à jour un environnement d'exécution	Écrire	Environment*		

Types de ressources définis par le service de modernisation AWS du mainframe

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Application	`arn:${Partition}:m2:${Region}:${Account}:app/${ApplicationId}`	aws:ResourceTag/${TagKey}
Environment	`arn:${Partition}:m2:${Region}:${Account}:env/${EnvironmentId}`	aws:ResourceTag/${TagKey}

Clés de condition pour le AWS service de modernisation des ordinateurs centraux

AWS Le service de modernisation du mainframe définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour Amazon Managed Blockchain

Amazon Managed Blockchain (préfixe de service : `managedblockchain`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Managed Blockchain
- Types de ressources définis par Amazon Managed Blockchain
- Clés de condition pour Amazon Managed Blockchain

Actions définies par Amazon Managed Blockchain

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAccessor	Accorde l'autorisation de créer un réseau Amazon Managed Blockchain	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMember	Accorde l'autorisation de créer un membre d'un réseau Amazon Managed Blockchain	Écriture	network*		iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetwork	Accorde l'autorisation de créer un réseau Amazon Managed Blockchain	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateNode	Accorde l'autorisation de créer un nœud au sein d'un membre d'un réseau Amazon Managed Blockchain	Écriture	member		iam:CreateServiceLinkedRole
			network		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateProposal	Accorde l'autorisation de créer une proposition sur laquelle d'autres membres du réseau blockchain peuvent voter pour ajouter ou supprimer un membre sur un réseau Amazon Managed Blockchain	Écrire	network*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccessor	Accorde l'autorisation de créer un réseau Amazon Managed Blockchain	Écrire	accessor*		
DeleteMember	Accorde l'autorisation de supprimer un membre et toutes les ressources associées à partir d'un réseau Amazon Managed Blockchain	Écriture	member*		
DeleteNode	Accorde l'autorisation de supprimer un nœud d'un membre d'un réseau Amazon Managed Blockchain	Écrire	node*		
GET [autorisation uniquement]	Accorde l'autorisation d'envoyer des requêtes HTTP GET à un nœud Ethereum	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccessor	Accorde l'autorisation de renvoyer des informations détaillées sur un réseau Amazon Managed Blockchain	Lecture	accessor*		
GetMember	Accorde l'autorisation de renvoyer des informations détaillées sur un membre d'un réseau Amazon Managed Blockchain	Lecture	member*		
GetNetwork	Accorde l'autorisation de renvoyer des informations détaillées sur un réseau Amazon Managed Blockchain	Lecture	network*		
GetNode	Accorde l'autorisation de renvoyer des informations détaillées sur un nœud au sein d'un membre d'un réseau Amazon Managed Blockchain	Lecture	node*		
GetProposal	Accorde l'autorisation de renvoyer des informations détaillées sur une proposition d'un réseau Amazon Managed Blockchain	Lecture	proposal*		
Invoke [autorisation uniquement]	Accorde l'autorisation de créer WebSocket des connexions à un nœud Ethereum	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InvokeRpcBitcoinMainnet	Accorde l'autorisation d'invoquer le réseau principal Bitcoin RPCs	Lecture			
InvokeRpcBitcoinTestnet	Accorde l'autorisation d'invoquer le Bitcoin Testnet RPCs	Lecture			
InvokeRpcPolygonMainnet	Accorde l'autorisation d'invoquer le réseau principal de polygones RPCs	Lecture			
InvokeRpcPolygonMumbaiTestnet	Accorde l'autorisation d'invoquer le réseau de test Polygon Mumbai RPCs	Lecture			
ListAccessors	Octroie l'autorisation de répertorier les accesseurs Amazon Managed Blockchain détenus par le Compte AWS	List			
ListInvitations	Accorde l'autorisation de répertorier les invitations adressées aux actifs Compte AWS depuis n'importe quel réseau Managed Blockchain	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMembers	Accorde l'autorisation de répertorier les membres d'un réseau Amazon Managed Blockchain et les propriétés de leurs abonnements	List	network*		
ListNetworks	Accorde l'autorisation de répertorier les réseaux Amazon Managed Blockchain auxquels le courant Compte AWS participe	List			
ListNodes	Accorde l'autorisation de répertorier les nœuds au sein d'un membre d'un réseau Amazon Managed Blockchain	Liste	member network		
ListProposalVotes	Accorde l'autorisation de répertorier tous les votes pour une proposition, y compris la valeur du vote et l'identifiant unique du membre qui vote pour le réseau Amazon Managed Blockchain spécifique	Lecture	proposal*		
ListProposals	Accorde l'autorisation de répertorier des propositions pour le réseau Amazon Managed Blockchain spécifique	Liste	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation d'afficher les balises associées à une ressource Amazon Managed Blockchain	Lecture	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
POST [autorisation uniquement]	Accorde l'autorisation d'envoyer des requêtes HTTP POST à un nœud Ethereum	Gestion des autorisations			
RejectInvitation	Accorde l'autorisation de refuser l'invitation à rejoindre le réseau blockchain	Écriture	invitation*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource Amazon Managed Blockchain	Balisage	accessor		
			invitation		
			member		
			network		
			node		
			proposal		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource Amazon Managed Blockchain	Balisage	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys	
UpdateMember	Accorde l'autorisation de mettre à jour un membre d'un réseau Amazon Managed Blockchain	Écriture	member*		iam:CreateServiceLinkedRole
UpdateNode	Accorde l'autorisation de mettre à jour un nœud d'un membre d'un réseau Amazon Managed Blockchain	Écriture	node*		iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
VoteOnProposal	Accorde l'autorisation de voter pour une proposition au nom du membre du réseau blockchain spécifié	Écriture	proposal*		

Types de ressources définis par Amazon Managed Blockchain

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
network	`arn:${Partition}:managedblockchain:${Region}::networks/${NetworkId}`	aws:ResourceTag/${TagKey}
member	`arn:${Partition}:managedblockchain:${Region}:${Account}:members/${MemberId}`	aws:ResourceTag/${TagKey}
node	`arn:${Partition}:managedblockchain:${Region}:${Account}:nodes/${NodeId}`	aws:ResourceTag/${TagKey}
proposal	`arn:${Partition}:managedblockchain:${Region}::proposals/${ProposalId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
invitation	`arn:${Partition}:managedblockchain:${Region}:${Account}:invitations/${InvitationId}`	aws:ResourceTag/${TagKey}
accessor	`arn:${Partition}:managedblockchain:${Region}:${Account}:accessors/${AccessorId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Managed Blockchain

Amazon Managed Blockchain définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction des balises qui sont transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des balises associées à une ressource Amazon Managed Blockchain	Chaîne
aws:TagKeys	Filtre les actions en fonction des clés de balise qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Managed Blockchain Query

Amazon Managed Blockchain Query (préfixe de service : `managedblockchain-query`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Managed Blockchain Query
- Types de ressources définis par Amazon Managed Blockchain Query
- Clés de condition pour Amazon Managed Blockchain Query

Actions définies par Amazon Managed Blockchain Query

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetTokenBalance	Autorise les appels par lots pour GetTokenBalance l'API	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAssetContract	Accorde l'autorisation de récupérer des informations sur un contrat sur la blockchain.	Lecture			
GetTokenBalance	Octroie l'autorisation de récupérer le solde d'un jeton pour une adresse sur la blockchain.	Lecture			
GetTransaction	Octroie l'autorisation de récupérer une transaction sur la blockchain.	Lecture			
ListAssetContracts	Accorde l'autorisation de récupérer plusieurs contrats sur la blockchain.	List			
ListFilteredTransactionEvents	Autorise la récupération d'événements sur la blockchain avec des filtres supplémentaires	List			
ListTokenBalances	Octroie l'autorisation de récupérer plusieurs soldes sur la blockchain.	List			
ListTransactionEvents	Octroie l'autorisation de récupérer des événements dans une transaction sur la blockchain.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTransactions	Octroie l'autorisation de récupérer plusieurs transactions sur la blockchain.	List			

Types de ressources définis par Amazon Managed Blockchain Query

Amazon Managed Blockchain Query ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une instruction de politique IAM. Pour autoriser l'accès à Amazon Managed Blockchain Query, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour Amazon Managed Blockchain Query

Managed Blockchain Query ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des instructions de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Managed Grafana

Amazon Managed Grafana (préfixe de service : `grafana`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Managed Grafana

- Types de ressources définis par Amazon Managed Grafana
- Clés de condition pour Amazon Managed Grafana

Actions définies par Amazon Managed Grafana

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateLicense	Accorde l'autorisation de mettre à niveau un espace de travail avec une licence	Écriture	workspace*		aws-marketplace:ViewSubscriptions
CreateWorkspace	Accorde l'autorisation de créer un espace de travail	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceL

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					inkedRole organizations:DescribeOrganization sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions sso:GetSharedSsoConfiguration
CreateWorkspaceApiKey	Accorde l'autorisation de créer des clés API pour un espace de travail	Écrire	workspace*		
CreateWorkspaceServiceAccount	Accorde l'autorisation de créer des comptes de service pour un espace de travail	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkspaceServiceAccountToken	Accorde l'autorisation de créer des jetons de compte de service pour un espace de travail	Écrire	workspace*		
DeleteWorkspace	Accorde l'autorisation de supprimer un espace de travail.	Écrire	workspace*		sso:DeleteManagedApplicationInstance
DeleteWorkspaceApiKey	Accorde l'autorisation de supprimer des clés API d'un espace de travail	Écrire	workspace*		
DeleteWorkspaceServiceAccount	Accorde l'autorisation de supprimer des comptes de service pour un espace de travail	Écrire	workspace*		
DeleteWorkspaceServiceAccountToken	Accorde l'autorisation de supprimer des jetons de compte de service pour un espace de travail	Écrire	workspace*		
DescribeWorkspace	Accorde l'autorisation de décrire un espace de travail.	Lecture	workspace*		
DescribeWorkspaceAuthentication	Accorde l'autorisation de décrire les fournisseurs d'authentification sur un espace de travail	Lecture	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWorkspaceConfiguration	Autorise la description de la chaîne actuelle de configuration pour l'espace de travail	Lecture	workspace*		
DisassociateLicense	Accorde l'autorisation de supprimer une licence d'un espace de travail	Écriture	workspace*		
ListPermissions	Accorde l'autorisation de répertorier les autorisations sur un espace de travail	List	workspace*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications associées à un espace de travail	Lecture	workspace		
ListVersions	Octroie l'autorisation de répertorier toutes les versions de Grafana prises en charge disponibles. Vous pouvez également inclure un espace de travail pour répertorier les versions vers lesquelles la mise à niveau est possible.	List	workspace		
ListWorkspaceServiceAccountTokens	Accorde l'autorisation de répertorier les jetons de compte de service pour un espace de travail	Lecture	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWorkspaceServiceAccounts	Accorde l'autorisation de répertorier les comptes de service pour un espace de travail	Lecture	workspace*		
ListWorkspaces	Accorde l'autorisation de répertorier les espaces de travail.	Lecture			
TagResource	Accorde l'autorisation d'ajouter des identifications à un espace de travail ou de mettre à jour les valeurs des identifications de cet espace	Identification	workspace*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une identification d'un espace de travail	Identification	workspace*		
				aws:TagKeys	
UpdatePermissions	Accorde l'autorisation de modifier les autorisations sur un espace de travail	Gestion des autorisations	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateWorkspace	Accorde l'autorisation de modifier un espace de travail	Écrire	workspace*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole
UpdateWorkspaceAuthentication	Accorde l'autorisation de modifier les fournisseurs d'authentification sur un espace de travail	Écrire	workspace*		
UpdateWorkspaceConfiguration	Accorde l'autorisation de mettre à jour la chaîne de configuration pour l'espace de travail donné Workspace	Écrire	workspace*		

Types de ressources définis par Amazon Managed Grafana

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workspace	`arn:${Partition}:grafana:${Region}:${Account}:/workspaces/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Managed Grafana

Amazon Managed Grafana définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des actions basées sur la présence de paires clé-valeur de balise dans la requête	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des actions basées sur les paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des actions basées sur la présence de clés d'identification dans la requête	ArrayOfString

Actions, ressources et clés de condition pour Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus (préfixe de service : `aps`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Managed Service for Prometheus
- Types de ressources définis par Amazon Managed Service for Prometheus
- Clés de condition pour Amazon Managed Service for Prometheus

Actions définies par Amazon Managed Service for Prometheus

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAlertManagerAlerts	Accorde l'autorisation de créer des alertes	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CreateAlertManagerDefinition	Accorde l'autorisation de créer une définition de gestionnaire d'alertes	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
CreateAnomalyDetector	Accorde l'autorisation de créer un détecteur d'anomalies	Écrire	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggingConfiguration	Autorise la création d'un ensemble de configuration	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
CreateQueryLoggingConfiguration	Accorde l'autorisation de créer une configuration de journalisation des requêtes	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CreateRuleGroupsNamespace	Accorde l'autorisation de créer un espace de noms de groupes de règles	Écrire	rulegroupsnamespace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScraper	Octroie l'autorisation de créer un scraper.	Écrire	cluster*		aps:TagResource ec2:DescribeSecurityGroups ec2:DescribeSubnets eks:DescribeCluster iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workspace*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateWorkspace	Accorde l'autorisation de créer un espace de travail	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlertManagerDefinition	Accorde l'autorisation de supprimer une définition de gestionnaire d'alertes	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteAlertManagerSilence	Accorde l'autorisation de supprimer un silence	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteAnomalyDetector	Accorde l'autorisation de supprimer un détecteur d'anomalies	Écrire	anomalydetector*		
			workspace*		
				aws:ResourceTag/${TagKey}	
DeleteLoggingConfiguration	Accorde l'autorisation de supprimer un jeu de configuration	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteQueryLoggingConfiguration	Accorde l'autorisation de supprimer une configuration de journalisation des requêtes	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique de ressources de l'espace de travail	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteRuleGroupsNamespace	Accorde l'autorisation de supprimer un espace de noms de groupes de règles	Écrire	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DeleteScraper	Octroie l'autorisation de supprimer un scraper.	Écrire	scraper*		
				aws:ResourceTag/${TagKey}	
DeleteScraperLoggingConfiguration	Autorise la suppression d'une configuration de journalisation Scraper	Écrire	scraper*		
				aws:ResourceTag/${TagKey}	
DeleteWorkspace	Accorde l'autorisation de supprimer un espace de travail.	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAlertManagerDefinition	Accorde l'autorisation de décrire une définition de gestionnaire d'alertes	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeAnomalyDetector	Autorise la description d'un détecteur d'anomalies	Lecture	anomalydetector*		
			workspace*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingConfiguration	Accorde l'autorisation de décrire la configuration de journalisation d'un pare-feu	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeQueryLoggingConfiguration	Accorde l'autorisation de décrire une configuration de journalisation des requêtes	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeResourcePolicy	Accorde l'autorisation de décrire la politique des ressources de l'espace de travail	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeRuleGroupsNamespace	Accorde l'autorisation de décrire un espace de noms de groupes de règles	Lecture	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DescribeScraper	Octroie l'autorisation de décrire un scraper.	Lecture	scraper*		
				aws:ResourceTag/${TagKey}	
DescribeScraperLoggingConfiguration	Accorde l'autorisation de décrire une configuration de journalisation Scraper	Lecture	scraper*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspace	Accorde l'autorisation de décrire un espace de travail	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWorkspaceConfiguration	Accorde l'autorisation de décrire la configuration de l'espace de travail	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerSilence	Accorde l'autorisation d'obtenir un silence	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerStatus	Accorde l'autorisation d'obtenir l'état actuel d'un gestionnaire d'alertes	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
GetDefaultScraperConfiguration	Octroie l'autorisation d'obtenir la configuration par défaut du scraper.	Lecture			
GetLabels	Accorde l'autorisation de récupérer des étiquettes d'espace de travail AMP.	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMetricMetadata	Accorde l'autorisation de récupérer les métadonnées pour les métriques de l'espace de travail AMP.	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
GetSeries	Accorde l'autorisation de récupérer des données de séries temporelles de l'espace de travail AMP.	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlertGroups	Accorde l'autorisation de répertorier des groupes	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlerts	Accorde l'autorisation de répertorier des alertes	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerReceivers	Accorde l'autorisation de répertorier des récepteurs	Lecture	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ListAlertManagerSilences	Accorde l'autorisation de répertorier des silences	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlerts	Accorde l'autorisation de répertorier des alertes actives	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
ListAnomalyDetectors	Permet de répertorier les détecteurs d'anomalies	List	workspace*		
				aws:ResourceTag/${TagKey}	
ListRuleGroupsNamespaces	Octroie l'autorisation de répertorier des espaces de noms de groupes de règles	List	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRules	Accorde l'autorisation de répertorier des règles d'alerte et d'enregistrement	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
ListScrapers	Octroie l'autorisation de répertorier les scrapers.	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises sur une ressource AMP	Lecture	anomalydetector		
			rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
ListWorkspaces	Accorde l'autorisation de répertorier les espaces de travail.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PreviewAnomalyDetector	Accorde l'autorisation de prévisualiser la détection des anomalies sur les métriques de l'espace de travail AMP	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
PutAlertManagerDefinition	Accorde l'autorisation de mettre à jour une définition de gestionnaire d'alertes	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
PutAlertManagerSilences	Accorde l'autorisation de créer ou de mettre à jour un silence	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
PutAnomalyDetector	Accorde l'autorisation de mettre à jour un détecteur d'anomalies	Écrire	anomalydetector*		
			workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutResourcePolicy	Autorise la création et la mise à jour de la politique des ressources de l'espace de travail	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
PutRuleGroupsNamespace	Accorde l'autorisation de mettre à jour un espace de noms de groupes de règles	Écrire	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
QueryMetrics	Accorde l'autorisation d'exécuter une requête sur les métriques de l'espace de travail AMP	Lecture	workspace*		
				aws:ResourceTag/${TagKey}	
RemoteWrite	Accorde l'autorisation d'exécuter une opération d'écriture à distance pour lancer le streaming de métriques de l'espace de travail AMP.	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource AMP	Identification	anomalydetector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource AMP	Identification	anomalydetector		
			rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys	
UpdateLoggingConfiguration	Accorde l'autorisation de mettre à jour une configuration de journal en temps réel	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateQueryLoggingConfiguration	Autorise la mise à jour d'une configuration de journalisation des requêtes	Écrire	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateScraper	Autorise la mise à jour d'un scraper	Écrire	scraper*		aps:CreateScraper aps:TagResource
			workspace		
				aws:ResourceTag/${TagKey}	
UpdateScraperLoggingConfiguration	Autorise la mise en place d'une configuration de journalisation Scraper	Écrire	scraper*		
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceAlias	Accorde l'autorisation de modifier l'alias de l'espace de travail AMP existante.	Écrire	workspace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceConfiguration	Autorise à mettre à jour la configuration de l'espace de travail	Écrire	workspace *		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon Managed Service for Prometheus

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workspace	`arn:${Partition}:aps:${Region}:${Account}:workspace/${WorkspaceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Types de ressources	ARN	Clés de condition
rulegroupsnamespace	arn:${Partition}:aps:${Region}:${Account}:rulegroupsnamespace/${WorkspaceId}/${Namespace}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
anomalydetector	arn:${Partition}:aps:${Region}:${Account}:anomalydetector/${WorkspaceId}/${AnomalyDetectorId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
scraper	arn:${Partition}:aps:${Region}:${Account}:scraper/${ScraperId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka (préfixe de service : `kafka`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Managed Streaming for Apache Kafka
- Types de ressources définis par Amazon Managed Streaming for Apache Kafka
- Clés de condition pour Amazon Managed Streaming for Apache Kafka

Actions définies par Amazon Managed Streaming for Apache Kafka

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchAssociateScramSecret	Accorde l'autorisation d'associer un ou plusieurs Scram Secrets à un cluster Amazon MSK.	Écriture	cluster*		kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecret	Accorde l'autorisation de dissocier un ou plusieurs Scram Secrets d'un cluster Amazon MSK.	Écriture	cluster*		kms:RetireGrant
CreateCluster	Accorde l'autorisation de créer un cluster MSK.	Écrire	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateClusterV2	Accorde l'autorisation de créer un cluster MSK.	Écriture	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	Accorde l'autorisation de créer une configuration MSK.	Écrire	configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReplicator	Accorde l'autorisation de créer un réplicateur MSK.	Écrire	replicator*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy kafka:DescribeClusterV2 kafka:GetBootstrapBrokers

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopic	Accorde l'autorisation de créer un sujet Kafka dans un cluster MSK	Écrire	topic*		kafka-cluster:Connect kafka-cluster:CreateTopic

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateVpcConnection	Accorde l'autorisation de créer une connexion MSK VPC	Écrire	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:PutRolePolicy
			vpc-connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Accorde l'autorisation de supprimer un cluster MSK.	Écrire	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints
DeleteClusterPolicy	Accorde l'autorisation de supprimer une politique basée sur les ressources du cluster	Écrire	cluster*		
DeleteConfiguration	Accorde l'autorisation de supprimer la configuration MSK spécifiée.	Écrire	configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteReplicator	Accorde l'autorisation de supprimer un réplicateur MSK.	Écrire	replicator*		
DeleteTopic	Accorde l'autorisation de supprimer un sujet Kafka d'un cluster MSK	Écrire	topic*		kafka-cluster:Connect kafka-cluster:DeleteTopic kafka-cluster:DescribeTopic
DeleteVpcConnection	Accorde l'autorisation de supprimer une connexion MSK VPC	Écrire	vpc-connection*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DescribeCluster	Accorde l'autorisation de décrire un cluster MSK.	Lecture	cluster*		
DescribeClusterOperation	Accorde l'autorisation de décrire l'opération de cluster spécifiée par l'ARN donné.	Lecture			
DescribeClusterOperationV2	Accorde l'autorisation de décrire l'opération de cluster spécifiée par l'ARN donné.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeClusterV2	Accorde l'autorisation de décrire un cluster MSK.	Lecture	cluster*		
DescribeConfiguration	Accorde l'autorisation de décrire une configuration MSK.	Lecture	configuration*		
DescribeConfigurationRevision	Accorde l'autorisation de décrire une révision de configuration MSK.	Lecture	configuration*		
DescribeReplicator	Accorde l'autorisation de décrire un réplicateur MSK.	Lecture	replicator*		
DescribeTopic	Accorde l'autorisation de renvoyer les détails des métadonnées concernant un sujet Kafka spécifique	Lecture	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic kafka-cluster:DescribeTopicDynamicConfiguration

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTopicPartitions	Accorde l'autorisation de répertorier toutes les partitions d'un sujet spécifique	Lecture	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic kafka-cluster:DescribeTopicDynamicConfiguration
DescribeVpcConnection	Accorde l'autorisation de décrire une connection MSK VPC	Lecture	vpc-connection*		
GetBootstrapBrokers	Accorde l'autorisation d'obtenir des informations de connexion pour les agents dans un cluster MSK.	Lecture			
GetClusterPolicy	Accorde l'autorisation de décrire une politique basée sur les ressources du cluster	Lecture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCompatibleKafkaVersions	Accorde l'autorisation d'obtenir une liste des versions d'Apache Kafka vers lesquelles vous pouvez mettre à jour un cluster MSK.	List			
ListClientVpcConnections	Accorde l'autorisation de répertorier toutes les connexions MSK VPC créées pour un cluster	List	cluster*		
ListClusterOperations	Accorde l'autorisation de renvoyer une liste de toutes les opérations qui ont été effectuées sur le cluster MSK spécifié	List	cluster*		
ListClusterOperationsV2	Accorde l'autorisation de renvoyer une liste de toutes les opérations qui ont été effectuées sur le cluster MSK spécifié	Liste	cluster*		
ListClusters	Accorde l'autorisation de répertorier tous les clusters MSK dans ce compte.	List			
ListClustersV2	Accorde l'autorisation de répertorier tous les clusters MSK dans ce compte.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConfigurationRevisions	Accorde l'autorisation de répertorier toutes les révisions pour une configuration MSK dans ce compte.	Liste	configuration*		
ListConfigurations	Accorde l'autorisation de répertorier toutes les configurations MSK dans ce compte.	Liste			
ListKafkaVersions	Accorde l'autorisation de répertorier toutes les versions d'Apache Kafka prises en charge par Amazon MSK.	Liste			
ListNodes	Accorde l'autorisation de répertorier des agents dans un cluster MSK.	List	cluster*		
ListReplicators	Accorde l'autorisation de répertorier tous les réplicateurs MSK dans ce compte.	List			
ListScramSecrets	Accorde l'autorisation de répertorier des Secrets Scram associés à un cluster Amazon MSK.	Liste	cluster*		
ListTagsForResource	Accorde l'autorisation de répertorier des balises d'une ressource MSK.	Lecture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTopics	Accorde l'autorisation de répertorier tous les sujets Kafka pour un cluster MSK spécifié	List	cluster*		kafka-cluster:Connect kafka-cluster:DescribeTopic
ListVpcConnections	Accorde l'autorisation de répertorier toutes les connexions MSK VPC utilisées par ce compte	List			
PutClusterPolicy	Accorde l'autorisation de créer ou de mettre à jour la politique basée sur les ressources du cluster	Écrire	cluster*		
RebootBroker	Accorde l'autorisation de redémarrer l'agent.	Écrire	cluster*		
RejectClientVpcConnection	Accorde l'autorisation de rejeter une connexion MSK VPC	Écrire	cluster*		
			vpc-connection*		
TagResource	Accorde l'autorisation de baliser une ressource MSK.	Balisage	cluster		
			vpc-connection		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource MSK.	Balisage	cluster		
			vpc-connection		
				aws:TagKeys	
UpdateBrokerCount	Accorde l'autorisation de mettre à jour le nombre d'agents du cluster MSK	Écriture	cluster*		
UpdateBrokerStorage	Accorde l'autorisation de mettre à jour la taille de stockage des agents du cluster MSK	Écriture	cluster*		
UpdateBrokerType	Accorde l'autorisation de mettre à jour le type d'agent d'un cluster Amazon MSK	Écriture	cluster*		
UpdateClusterConfiguration	Accorde l'autorisation de mettre à jour la configuration du cluster MSK.	Écriture	cluster*		
			configuration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateClusterKafkaVersion	Accorde l'autorisation de mettre à jour le cluster MSK vers la version d'Apache Kafka spécifiée.	Écriture	cluster*		
UpdateConfiguration	Accorde l'autorisation de créer une nouvelle révision de la configuration MSK.	Écrire	configuration*		
UpdateConnectivity	Accorde l'autorisation de mettre à jour les paramètres de connectivité pour le cluster MSK.	Écrire	cluster*		ec2:DescribeRouteTables ec2:DescribeSubnets
				kafka:publicAccessEnabled	
UpdateMonitoring	Accorde l'autorisation de mettre à jour les paramètres de surveillance pour le cluster MSK.	Écrire	cluster*		
UpdateRebalancing	Autorise la mise à jour de l'état de rééquilibrage intelligent du cluster MSK	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateReplicationInfo	Accorde l'autorisation de mettre à jour les informations de réplication du réplicateur MSK.	Écrire	replicator*		
UpdateSecurity	Accorde l'autorisation de mettre à jour les paramètres de sécurité pour le cluster MSK.	Écrire	cluster*		kms:RetireGrant
UpdateStorage	Accorde l'autorisation de mettre à jour le stockage EBS (taille ou débit alloué) associé aux agents MSK ou de définir le mode de stockage des clusters sur TIERED	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTopic	Accorde l'autorisation de mettre à jour la configuration d'un sujet Kafka dans un cluster MSK	Écrire	topic*		kafka-cluster:AlterTopic kafka-cluster:AlterTopicDynamicConfiguration kafka-cluster:Connect kafka-cluster:DescribeTopic

Types de ressources définis par Amazon Managed Streaming for Apache Kafka

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${Uuid}	aws:ResourceTag/${TagKey}
configuration	arn:${Partition}:kafka:${Region}:${Account}:configuration/${ConfigurationName}/${Uuid}	
vpc-connection	arn:${Partition}:kafka:${Region}:${VpcOwnerAccount}:vpc-connection/${ClusterOwnerAccount}/${ClusterName}/${Uuid}	aws:ResourceTag/${TagKey}
replicator	arn:${Partition}:kafka:${Region}:${Account}:replicator/${ReplicatorName}/${Uuid}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}	
group	arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}	
transactional-id	arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}	

Clés de condition pour Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour

affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
kafka:publicAccessEnabled	Filtre l'accès en fonction de la présence d'accès public activé dans la demande	Booléen

Actions, ressources et clés de condition pour Amazon Managed Streaming for Kafka Connect

Amazon Managed Streaming for Kafka Connect (préfixe de service : `kafkaconnect`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définie par Amazon Managed Streaming for Kafka Connect

- Types de ressources définis par Amazon Managed Streaming for Kafka Connect
- Clés de condition pour Amazon Managed Streaming for Kafka Connect

Actions définie par Amazon Managed Streaming for Kafka Connect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConnector	Accorde l'autorisation de créer un connecteur MSK Connect	Écrire			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs firehose:TagDeliveryStream

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy logs:CreateLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					logs:ListLogDeliveries logs:PutResourcePolicy s3:GetBucketPolicy s3:PutBucketPolicy
CreateCustomPlugin	Accorde l'autorisation de créer un plugin personnalisé MSK Connect	Écrire			s3:GetObject
CreateWorkerConfiguration	Accorde l'autorisation de créer une configuration d'environnement de travail MSK Connect	Écrire			
DeleteConnector	Accorde l'autorisation de supprimer un connecteur MSK Connect	Écrire	connector*		logs:DeleteLogDelivery logs:ListLogDeliveries

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCustomPlugin	Accorde l'autorisation de supprimer un plugin personnalisé MSK Connect	Écrire	custom plugin*		
DeleteWorkerConfiguration	Accorde l'autorisation de supprimer une configuration de travail MSK Connect	Écrire	worker configuration*		
DescribeConnector	Accorde l'autorisation de décrire un connecteur MSK Connect	Lecture	connector*		
DescribeConnectorOperation	Accorde l'autorisation de décrire le fonctionnement d'un connecteur MSK Connect	Lecture	connector operation*		
DescribeCustomPlugin	Accorde l'autorisation de décrire un plugin personnalisé MSK Connect	Lecture	custom plugin*		
DescribeWorkerConfiguration	Accorde l'autorisation de décrire une configuration d'environnement de travail MSK Connect	Lecture	worker configuration*		
ListConnectorOperations	Permet de répertorier toutes les opérations d'un connecteur MSK Connect donné	Lecture	connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConnectors	Accorde l'autorisation de répertorier tous les connecteurs MSK Connect dans ce compte.	Lecture			
ListCustomPlugins	Accorde l'autorisation de répertorier tous les plugins personnalisés MSK Connect dans ce compte.	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource MSK Connect	Lecture	connector	aws:ResourceTag/${TagKey}	
			custom plugin	aws:ResourceTag/${TagKey}	
			worker configuration	aws:ResourceTag/${TagKey}	
ListWorkerConfigurations	Accorde l'autorisation de répertorier toutes les configuration d'environnement de travail MSK Connect dans ce compte.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser une ressource MSK Connect	Identification	connector	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			custom plugin	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			worker configuration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource MSK Connect	Identification	connector	aws:TagKeys	
			custom plugin	aws:TagKeys	
			worker configuration	aws:TagKeys	
				aws:TagKeys	
UpdateConnector	Accorde l'autorisation de mettre à jour un connecteur MSK Connect	Écrire	connector*		

Types de ressources définis par Amazon Managed Streaming for Kafka Connect

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
connector	`arn:${Partition}:kafkaconnect:${Region}:${Account}:connector/${ConnectorName}/${UUID}`	aws:ResourceTag/${TagKey}
custom plugin	`arn:${Partition}:kafkaconnect:${Region}:${Account}:custom-plugin/${CustomPluginName}/${UUID}`	aws:ResourceTag/${TagKey}
worker configuration	`arn:${Partition}:kafkaconnect:${Region}:${Account}:worker-configuration/${WorkerConfigurationName}/${UUID}`	aws:ResourceTag/${TagKey}
connector operation	`arn:${Partition}:kafkaconnect:${Region}:${Account}:connector-operation/${ConnectorName}/${ConnectorUUID}/${UUID}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Managed Streaming for Kafka Connect

Amazon Managed Streaming for Kafka Connect définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow (préfixe de service : `airflow`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Managed Workflows for Apache Airflow
- Types de ressources définies par Amazon Managed Workflows for Apache Airflow
- Clés de condition pour Amazon Managed Workflows for Apache Airflow

Actions définies par Amazon Managed Workflows for Apache Airflow

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCliToken	Accorde l'autorisation de créer un jeton de courte durée permettant à un utilisateur d'appeler Airflow CLI via un point de terminaison sur le serveur web Apache Airflow.	Écriture	environment*		
CreateEnvironment	Accorde l'autorisation de créer un environnement Amazon MWAA.	Écriture	environment*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebLoginToken	Accorde l'autorisation de créer un jeton de courte durée permettant à un utilisateur de se connecter à l'interface utilisateur web Apache Airflow.	Écriture	rbac-role*		
DeleteEnvironment	Accorde l'autorisation de supprimer un environnement Amazon MWAA.	Écriture	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetEnvironment	Accorde l'autorisation d'afficher des informations relatives à un environnement Amazon MWAA	Lecture	environment*		
				aws:ResourceTag/${TagKey}	
InvokeRestApi	Accorde l'autorisation d'invoquer l'API REST Airflow via un point de terminaison sur le serveur Web Apache Airflow	Écrire	rbac-role*		
ListEnvironments	Accorde l'autorisation de répertorier les environnements Amazon MWAA dans votre compte.	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour un environnement Amazon MWAA.	Lecture	environment		
				aws:ResourceTag/${TagKey}	
PublishMetrics	Accorde l'autorisation de publier des métriques pour un environnement Amazon MWAA.	Écriture	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser un environnement Amazon MWAA.	Balisage	environment		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'un environnement Amazon MWAA.	Balisage	environment		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateEnvironment	Accorde l'autorisation de modifier un environnement Amazon MWAA.	Écriture	environment*		
				aws:ResourceTag/${TagKey}	

Types de ressources définies par Amazon Managed Workflows for Apache Airflow

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
environment	`arn:${Partition}:airflow:${Region}:${Account}:environment/${EnvironmentName}`	
rbac-role	`arn:${Partition}:airflow:${Region}:${Account}:role/${EnvironmentName}/${RoleName}`	

Clés de condition pour Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString

Actions, ressources et clés de condition pour AWS Marketplace

AWS Marketplace (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace
- Types de ressources définis par AWS Marketplace
- Clés de condition pour AWS Marketplace

Actions définies par AWS Marketplace

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptAgreementApprovalRequest	Accorde l'autorisation aux utilisateurs d'approuver une demande d'abonnement entrante (pour les fournisseurs qui fournissent des produits nécessitant une vérification d'abonnement)	Écrire			
AcceptAgreementCancellationRequest	Autorise les utilisateurs à accepter une demande d'annulation d'accord	Écrire			
AcceptAgreementPaymentRequest	Autorise les utilisateurs à accepter une demande de paiement	Écrire			
AcceptAgreementRequest	Autorise les utilisateurs à accepter leurs demandes d'accord	Écrire			
BatchCreateBillingAdjustmentRequest	Autorise les utilisateurs à créer une demande d'ajustement de facturation dans le cadre d'un accord	Écrire			
CancelAgreement	Autorise les utilisateurs à annuler leurs accords	Écrire			
CancelAgreementCan	Autorise les utilisateurs à retirer une demande d'annulation d'accord en attente	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
cellation Request					
CancelAgreementPaymentRequest	Autorise les utilisateurs à annuler une demande de paiement	Écrire			
CancelAgreementRequest	Accorde aux utilisateurs l'autorisation d'annuler les demandes d'abonnement en attente pour les produits nécessitant une vérification d'abonnement	Écrire			
CreateAgreementRequest	Autorise les utilisateurs à créer une demande d'accord	Écrire			
DescribeAgreement	Autorise les utilisateurs à décrire les métadonnées relatives à l'accord	Lecture			
GetAgreementApprovalRequest	Accorde l'autorisation d'afficher les détails de leurs demandes d'abonnement entrantes (pour les fournisseurs qui fournissent des produits nécessitant une vérification d'abonnement)	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAgreementCancellationRequest	Autorise les utilisateurs à consulter les détails d'une demande d'annulation d'accord	Lecture			
GetAgreementEntitlements	Autorise les utilisateurs à consulter les droits associés à un accord	Lecture			
GetAgreementPaymentRequest	Autorise les utilisateurs à consulter les détails d'une demande de paiement	Lecture			
GetAgreementRequest	Accorde aux utilisateurs l'autorisation d'afficher les détails de leurs demandes d'abonnement pour les produits de données nécessitant une vérification d'abonnement	Lecture			
GetAgreementTerms	Accorde l'autorisation d'obtenir une liste de conditions pour un accord	List			
GetBillingAdjustmentRequest	Autorise les utilisateurs à consulter les détails d'une demande d'ajustement de facturation	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAgreementApprovalRequests	Accorde l'autorisation aux utilisateurs de répertorier leurs demandes d'abonnement entrantes (pour les fournisseurs qui fournissent des produits nécessitant une vérification d'abonnement)	List			
ListAgreementCancellationRequests	Autorise les utilisateurs à répertorier les demandes d'annulation d'accord	List			
ListAgreementCharges	Autorise les utilisateurs à consulter les frais associés à leurs contrats	List			
ListAgreementInvoiceLineItems	Autorise les utilisateurs à répertorier les éléments de facture d'un accord	List			
ListAgreementPaymentRequests	Autorise les utilisateurs à répertorier les demandes de paiement pour un accord	List			
ListAgreementRequests	Accorde aux utilisateurs l'autorisation de répertorier leurs demandes d'abonnement pour les produits nécessitant une vérification d'abonnement.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBillingAdjustmentRequests	Autorise les utilisateurs à répertorier les demandes d'ajustement de facturation	List			
ListEntitlementDetails	Accorde l'autorisation aux utilisateurs de consulter les détails des droits associés à un accord. Remarquez que cette action ne s'applique pas aux achats Marketplace	Lecture			
RejectAgreementApprovalRequest	Accorde l'autorisation aux utilisateurs de refuser une demande d'abonnement entrante (pour les fournisseurs qui fournissent des produits nécessitant une vérification d'abonnement)	Écrire			
RejectAgreementCancellationRequest	Autorise les utilisateurs à rejeter une demande d'annulation d'accord	Écrire			
RejectAgreementPaymentRequest	Autorise les utilisateurs à rejeter une demande de paiement	Écrire			
SearchAgreements	Autorise les utilisateurs à effectuer des recherches sur leurs accords	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendAgreementCancellationRequest	Autorise les utilisateurs à envoyer une demande d'annulation d'accord	Écrire			
SendAgreementPaymentRequest	Autorise les utilisateurs à envoyer une demande de paiement	Écrire			
Subscribe	Autorise les utilisateurs à s'abonner à AWS Marketplace des produits. Inclut la possibilité d'envoyer une demande d'abonnement pour les produits nécessitant une vérification d'abonnement. Inclut la possibilité d'activer le renouvellement automatique d'un abonnement existant	Écrire			
Unsubscribe	Autorise les utilisateurs à supprimer les abonnements aux AWS Marketplace produits. Inclut la possibilité de désactiver le renouvellement automatique d'un abonnement existant	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgreementApprovalRequest	Accorde aux utilisateurs l'autorisation d'apporter des modifications à une demande d'abonnement entrante, y compris la possibilité de supprimer les informations de l'abonné potentiel (pour les fournisseurs qui fournissent des produits nécessitant une vérification d'abonnement)	Écrire			
UpdatePurchaseOrders	Autorise les utilisateurs à mettre à jour les bons de commande pour les frais associés à leurs contrats	Écrire			
ViewSubscriptions	Autorise les utilisateurs à voir les abonnements de leur compte	List			

Types de ressources définis par AWS Marketplace

AWS Marketplace ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Marketplace

AWS Marketplace définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws-marketplace:AgreementType	Filtre l'accès en fonction du type de l'accord	ArrayOfString
aws-marketplace:PartyType	Filtre l'accès en fonction du type de partie de l'accord	String
aws-marketplace:ProductId	Filtre l'accès par identifiant de produit pour AWS Marketplace RedHat OpenShift et pour les produits Bedrock. Remarque : L'utilisation de cette clé de condition ne limitera pas l'accès aux produits dans AWS Marketplace	ArrayOfString

Actions, ressources et clés de condition pour le AWS Marketplace catalogue

AWS Marketplace Le catalogue (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS Marketplace catalogue

- Types de ressources définis par le AWS Marketplace catalogue
- Clés de condition pour le AWS Marketplace catalogue

Actions définies par le AWS Marketplace catalogue

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelChangeSet	Accorde l'autorisation d'annuler un jeu de modifications en cours d'exécution	Écrire	ChangeSet*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique de ressource d'une entité existante	Gestion des autorisations	Entity*		
DescribeAssessment	Permet de renvoyer les détails d'une évaluation existante	Lecture	Assessment		
DescribeChangeSet	Accorde l'autorisation de renvoyer les détails d'un jeu de modifications existant	Lecture	ChangeSet*		
DescribeEntity	Accorde l'autorisation de renvoyer les détails d'une entité existante	Lecture	Entity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourcePolicy	Accorde l'autorisation d'obtenir la politique de ressource d'une entité existante	Lecture	Entity*		
ListAssessments	Donne l'autorisation de répertorier les évaluations existantes	List			
ListChangeSets	Accorde l'autorisation de répertorier les jeux de modifications existants	List			
ListEntities	Accorde l'autorisation de répertorier les entités existantes	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises sur une entité existante ou sur un jeu de modifications	Lecture	ChangeSet		
			Entity		
PutResourcePolicy	Accorde l'autorisation d'attacher une politique de ressource à une entité existante	Gestion des autorisations	Entity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartChangeSet	Accorde l'autorisation de demander un nouvel ensemble de modifications (Remarque : les autorisations au niveau des ressources pour cette action et les clés contextuelles de condition pour cette action ne sont prises en charge que lorsqu'elles sont utilisées avec l'API du catalogue et ne sont pas prises en charge avec le portail de AWS Marketplace gestion)	Écrire	Entity*		
				catalog:ChangeType aws-marketplace:Intent aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation de baliser une entité existante ou un jeu de modifications	Identification	ChangeSet		
			Entity		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les balises d'une entité existante ou d'un jeu de modifications	Identification	ChangeSet		
			Entity		
				aws:TagKeys	

Types de ressources définis par le AWS Marketplace catalogue

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Entity	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/${EntityType}/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType
ChangeSet	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/ChangeSet/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType
Assessment	`arn:${Partition}:aws-marketplace:${Region}::${Catalog}/Assessment/${ResourceId}`	

Clés de condition pour le AWS Marketplace catalogue

AWS Marketplace Le catalogue définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws-marketplace:Intent	Filtre l'accès en fonction du paramètre Intent dans la StartChangeSet demande	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
catalog:ChangeType	Filtre l'accès en fonction du type de modification indiqué dans la StartChangeSet demande	String

Actions, ressources et clés de condition pour AWS Marketplace le service Commerce Analytics

AWS Marketplace Commerce Analytics Service (préfixe de service :`marketplacecommerceanalytics`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

Rubriques

- Actions définies par le service d'analyse AWS Marketplace du commerce
- Types de ressources définis par AWS Marketplace Commerce Analytics Service
- Clés de condition pour le service d'analyse AWS Marketplace du commerce

Actions définies par le service d'analyse AWS Marketplace du commerce

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GenerateDataSet	Demandez la publication d'un jeu de données dans votre compartiment Amazon S3.	Écriture			
StartSupportDataExport	Demandez la publication d'un jeu de données de support dans votre compartiment Amazon S3.	Écrire			

Types de ressources définis par AWS Marketplace Commerce Analytics Service

AWS Marketplace Commerce Analytics Service ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Commerce Analytics Service, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le service d'analyse AWS Marketplace du commerce

CAS ne dispose pas de clés de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des instructions de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Marketplace le service de déploiement

AWS Marketplace Le service de déploiement (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service AWS Marketplace de déploiement
- Types de ressources définis par le service AWS Marketplace de déploiement
- Clés de condition pour AWS Marketplace le service de déploiement

Actions définies par le service AWS Marketplace de déploiement

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Octroie l'autorisation de répertorier les balises pour une ressource de paramètre de déploiement.	Lecture	DeploymentParameter		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
PutDeploymentParameter	Octroie l'autorisation de créer ou de mettre à jour une ressource de paramètre de déploiement.	Écrire	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	aws-marketplace:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Octroie l'autorisation de baliser une ressource de paramètre de déploiement.	Identification	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Octroie l'autorisation de retirer les balises d'une ressource de paramètre de déploiement.	Identification	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	

Types de ressources définis par le service AWS Marketplace de déploiement

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
DeploymentParameter	`arn:${Partition}:aws-marketplace:${Region}:${Account}:DeploymentParameter:catalogs/${CatalogName}/products/${ProductId}/${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Clés de condition pour AWS Marketplace le service de déploiement

AWS Marketplace Le service de déploiement définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner

les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Marketplace Discovery

AWS Marketplace Discovery (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace Discovery
- Types de ressources définis par AWS Marketplace Discovery
- Clés de condition pour AWS Marketplace Discovery

Actions définies par AWS Marketplace Discovery

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPrivateListings	Accorde l'autorisation aux utilisateurs de répertorier leurs offres privées	List			

Types de ressources définis par AWS Marketplace Discovery

AWS Marketplace Discovery ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Discovery, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Marketplace Discovery

Marketplace Discovery ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Marketplace Entitlement Service

AWS Marketplace Entitlement Service (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace Entitlement Service
- Types de ressources définis par AWS Marketplace Entitlement Service
- Clés de condition pour AWS Marketplace Entitlement Service

Actions définies par AWS Marketplace Entitlement Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEntitlements	Accorde l'autorisation de récupérer les valeurs d'autorisation pour un produit donné. Les résultats peuvent être filtrés en fonction de l'identifiant du client ou des dimensions du produit	Lecture			

Types de ressources définis par AWS Marketplace Entitlement Service

AWS Marketplace Entitlement Service ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Entitlement Service, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Marketplace Entitlement Service

Marketplace Entitlement ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Marketplace Image Building Service

AWS Marketplace Image Building Service (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace Image Building Service
- Types de ressources définis par AWS Marketplace Image Building Service
- Clés de condition pour AWS Marketplace Image Building Service

Actions définies par AWS Marketplace Image Building Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeBuilds [autorisation uniquement]	Décrit les générations d'image identifiées par un ID de génération	Lecture			
ListBuilds [autorisation uniquement]	Répertorie les générations d'images.	Lecture			
StartBuild [autorisation uniquement]	Démarre une génération d'image	Écrire			

Types de ressources définis par AWS Marketplace Image Building Service

AWS Marketplace Image Building Service ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Image Building Service, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Marketplace Image Building Service

Marketplace Image Build ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le portail AWS Marketplace de gestion

AWS Marketplace Le portail de gestion (préfixe de service :`aws-marketplace-management`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le portail AWS Marketplace de gestion
- Types de ressources définis par le portail AWS Marketplace de gestion
- Clés de condition pour le portail AWS Marketplace de gestion

Actions définies par le portail AWS Marketplace de gestion

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAdditionalSellerNotificationRecipients	Accorde l'autorisation d'afficher les destinataires supplémentaires des notifications sur les vendeurs.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
GetBankAccountVerificationDetails [autorisation uniquement]	Accorde l'autorisation d'afficher le statut de vérification du compte bancaire.	Lecture			
GetSecondaryUserVerificationDetails [autorisation uniquement]	Accorde l'autorisation d'afficher le statut de vérification du compte d'utilisateur secondaire.	Lecture			
GetSellerVerificationDetails [autorisation uniquement]	Accorde l'autorisation d'afficher le statut de vérification du compte.	Lecture			
PutAdditionalSellerNotificationRecipients [autorisation uniquement]	Accorde l'autorisation de mettre à jour les destinataires supplémentaires des notifications sur les vendeurs.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutBankAccountVerificationDetails [autorisation uniquement]	Accorde l'autorisation de mettre à jour le statut de vérification du compte bancaire.	Écrire			
PutSecondaryUserVerificationDetails [autorisation uniquement]	Accorde l'autorisation de mettre à jour le statut de vérification du compte d'utilisateur secondaire.	Écrire			
PutSellerVerificationDetails [autorisation uniquement]	Accorde l'autorisation de mettre à jour le statut de vérification du compte.	Écrire			
uploadFiles [autorisation uniquement]	Permet d'accéder à la page de téléchargement de fichiers dans le portail AWS Marketplace de gestion	Écrire			
viewMarketing [autorisation uniquement]	Permet d'accéder à la page Marketing dans le portail AWS Marketplace de gestion	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
viewReports [autorisation uniquement]	Permet d'accéder à la page Rapports dans le portail AWS Marketplace de gestion	List			
viewSettings [autorisation uniquement]	Permet d'accéder à la page des paramètres dans le portail AWS Marketplace de gestion	List			
viewSupport [autorisation uniquement]	Permet d'accéder à la page d'éligibilité au Support client dans le portail AWS Marketplace de gestion	List			

Types de ressources définis par le portail AWS Marketplace de gestion

AWS Marketplace Le portail de gestion ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Management Portal, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le portail AWS Marketplace de gestion

Le portail Marketplace ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le service AWS Marketplace de mesure

AWS Marketplace Le service de mesure (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS Marketplace service de mesure
- Types de ressources définis par le AWS Marketplace service de mesure
- Clés de condition pour le AWS Marketplace service de mesure

Actions définies par le AWS Marketplace service de mesure

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchMeterUsage	Accorde l'autorisation de publier des enregistrements de mesure pour un ensemble de clients pour les applications SaaS	Écriture			
MeterUsage	Accorde l'autorisation d'émettre des enregistrements de mesure	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterUsage	Accorde l'autorisation de vérifier que le client qui utilise votre logiciel payant est abonné à votre produit le AWS Marketplace, ce qui vous permet de vous prémunir contre toute utilisation non autorisée. Mesure l'utilisation du logiciel par tâche ECS, par heure, au prorata de l'utilisation par seconde	Écrire			
ResolveCustomer	Accorde l'autorisation de résoudre un jeton d'enregistrement pour obtenir un CustomerIdentifier code de produit	Écrire			

Types de ressources définis par le AWS Marketplace service de mesure

AWS Marketplace Le service de mesure ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Metering Service, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le AWS Marketplace service de mesure

Marketplace Metering ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Marketplace Private Marketplace

AWS Marketplace Private Marketplace (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace Private Marketplace
- Types de ressources définis par AWS Marketplace Private Marketplace
- Clés de condition pour AWS Marketplace Private Marketplace

Actions définies par AWS Marketplace Private Marketplace

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateProductsWithPrivateMarketplace	Accorde l'autorisation de créer une demande pour qu'un ou plusieurs produits soient associés à Private Marketplace. Cette action peut être	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]	effectuée par n'importe quel compte d'une AWS organisation, à condition que l'utilisateur soit autorisé à le faire et que les politiques de contrôle des services de l'organisation le permettent				
CreatePrivateMarketplaceRequests [autorisation uniquement]	Accorde l'autorisation de créer une demande pour qu'un ou plusieurs produits soient associés à Private Marketplace. Cette action peut être effectuée par n'importe quel compte au sein d'une AWS organisation, à condition que l'utilisateur soit autorisé à le faire et que les politiques de contrôle des services de l'organisation le permettent	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribePrivateMarketplaceRequests [autorisation uniquement]	Accorde l'autorisation de décrire les demandes et les produits associés dans Private Marketplace. Cette action peut être effectuée par n'importe quel compte d'une AWS organisation, à condition que l'utilisateur soit autorisé à le faire et que les politiques de contrôle des services de l'organisation le permettent	List			
DisassociateProductsFromPrivateMarketplace [autorisation uniquement]	Accorde l'autorisation de créer une demande pour qu'un ou plusieurs produits soient associés à Private Marketplace. Cette action peut être effectuée par n'importe quel compte d'une AWS organisation, à condition que l'utilisateur soit autorisé à le faire et que les politiques de contrôle des services de l'organisation le permettent	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPrivateMarketplaceRequests [autorisation uniquement]	Accorde l'autorisation d'obtenir une liste interrogeable pour les demandes et les produits associés dans Private Marketplace. Cette action peut être effectuée par n'importe quel compte d'une AWS organisation, à condition que l'utilisateur soit autorisé à le faire et que les politiques de contrôle des services de l'organisation le permettent	List			

Types de ressources définis par AWS Marketplace Private Marketplace

AWS Marketplace Private Marketplace ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Private Marketplace, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Marketplace Private Marketplace

Private Marketplace ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour l'intégration AWS Marketplace des systèmes d'approvisionnement

AWS Marketplace L'intégration des systèmes d'approvisionnement (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'intégration AWS Marketplace des systèmes d'approvisionnement
- Types de ressources définis par l'intégration AWS Marketplace des systèmes d'approvisionnement
- Clés de condition pour l'intégration AWS Marketplace des systèmes d'approvisionnement

Actions définies par l'intégration AWS Marketplace des systèmes d'approvisionnement

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeProcurementSystemConfiguration	Accorde l'autorisation de décrire la configuration d'intégration du système d'approvisionnement (par	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]	exemple Coupa) pour le compte individuel, ou pour l'ensemble de l' AWS organisation s'il en existe un. Cette action ne peut être effectuée par le compte principal que si vous utilisez une AWS organisation				
PutProcurementSystemConfiguration [autorisation uniquement]	Accorde l'autorisation de créer ou de mettre à jour la configuration d'intégration du système d'approvisionnement (par exemple Coupa) pour le compte individuel, ou pour l'ensemble de l' AWS organisation s'il en existe un. Cette action ne peut être effectuée par le compte principal que si vous utilisez une AWS organisation	Écrire			

Types de ressources définis par l'intégration AWS Marketplace des systèmes d'approvisionnement

AWS Marketplace L'intégration des systèmes d'approvisionnement ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Marketplace Procurement Systems Integration, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour l'intégration AWS Marketplace des systèmes d'approvisionnement

Marketplace Procurement Integration ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les AWS Marketplace rapports

AWS Marketplace Reporting (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace Reporting
- Types de ressources définis par AWS Marketplace Reporting
- Clés de condition pour les AWS Marketplace rapports

Actions définies par AWS Marketplace Reporting

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBuyerDashboard	Accorde l'autorisation de consulter un tableau de bord qui affiche les données AWS Marketplace d'achat d'un acheteur	Lecture	Dashboard *		

Types de ressources définis par AWS Marketplace Reporting

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Dashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Clés de condition pour les AWS Marketplace rapports

Marketplace Reporting ne possède aucune clé de contexte spécifique à un service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les rapports sur les AWS Marketplace vendeurs

AWS Marketplace Seller Reporting (préfixe de service :`aws-marketplace`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace Seller Reporting
- Types de ressources définis par AWS Marketplace Seller Reporting
- Clés de condition pour les rapports sur les AWS Marketplace vendeurs

Actions définies par AWS Marketplace Seller Reporting

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSellerDashboard	Accorde l'autorisation de consulter le tableau de bord d'un vendeur	Lecture	SellerDashboard*		

Types de ressources définis par AWS Marketplace Seller Reporting

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
SellerDashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Clés de condition pour les rapports sur les AWS Marketplace vendeurs

Les rapports Marketplace sur les vendeurs ne comportent aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights (préfixe de service :`vendor-insights`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Marketplace Vendor Insights
- Types de ressources définis par AWS Marketplace Vendor Insights
- Clés de condition pour AWS Marketplace Vendor Insights

Actions définies par AWS Marketplace Vendor Insights

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateSecurityProfile	Accorde l'autorisation d'activer le profil de sécurité	Écrire	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
AssociateDataSource	Accorde l'autorisation d'associer un profil de sécurité à une source de données	Écrire	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataSource	Accorde l'autorisation de créer une nouvelle source de données	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
CreateSecurityProfile	Accorde l'autorisation de créer un nouveau profil de sécurité	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
DeactivateSecurityProfile	Accorde l'autorisation de désactiver le profil de sécurité	Écrire	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Accorde l'autorisation de supprimer une source de données.	Écrire	DataSource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DisassociateDataSource	Accorde l'autorisation de dissocier un profil de sécurité à partir d'une source de données	Écrire	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
GetDataSource	Accorde l'autorisation de récupérer les détails d'une source de données existante	Lecture	DataSource*		
				aws:ResourceTag/${TagKey}	
GetEntitledSecurityProfileSnapshot	Accorde l'autorisation de renvoyer les détails d'un instantané de profil de sécurité que le demandeur est autorisé à lire	Lecture	SecurityProfile*		
GetProfileAccessTerms	Accorde l'autorisation d'obtenir les conditions d'accès pour un profil Vendor Insights	Lecture			
GetSecurityProfile	Accorde l'autorisation de renvoyer les détails d'un profil de sécurité existant	Lecture	SecurityProfile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetSecurityProfileSnapshot	Accorde l'autorisation de renvoyer les détails d'un instantané de profil de sécurité	Lecture	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Accorde l'autorisation de répertorier les sources de données existantes	List			
ListEntitledSecurityProfileSnapshots	Accorde l'autorisation de renvoyer la liste récapitulative des instantanés pour un profil de sécurité existant que le demandeur est autorisé à répertorier	List	SecurityProfile*		
ListEntitledSecurityProfiles	Accorde l'autorisation de répertorier les profils de sécurités autorisés	List			
ListSecurityProfileSnapshots	Accorde l'autorisation de renvoyer la liste récapitulative des instantanés pour un profil de sécurité existant	List	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSecurityProfiles	Accorde l'autorisation de répertorier les profils de sécurités existants	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource d'information sur les fournisseurs	Lecture	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser la ressource d'information sur les fournisseurs	Identification	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage de la ressource d'information sur les fournisseurs	Identification	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDataSource	Accorde l'autorisation de mettre à jour une source de données existante	Écrire	DataSource*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfile	Accorde l'autorisation de mettre à jour le profil de sécurité	Écrire	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotCreationConfiguration	Accorde l'autorisation de mettre à jour la configuration de la création d'instantané du profil de sécurité	Écrire	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSecurityProfileSnapshotReleaseConfiguration	Accorde l'autorisation de mettre à jour la configuration de la version d'instantané du profil de sécurité	Écrire	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS Marketplace Vendor Insights

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
DataSource	`arn:${Partition}:vendor-insights:::data-source:${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
SecurityProfile	`arn:${Partition}:vendor-insights:::security-profile:${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
		aws:TagKeys

Clés de condition pour AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le serveur AWS MCP

AWS Le serveur MCP (préfixe de service :`aws-mcp`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS serveur MCP
- Types de ressources définis par le AWS serveur MCP
- Clés de condition pour le AWS serveur MCP

Actions définies par le AWS serveur MCP

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CallReadOnlyTool	Accorde l'autorisation d'appeler des outils en lecture seule dans le service MCP	Lecture			
CallReadWriteTool	Autorise l'appel des API de AWS lecture et d'écriture dans le service MCP	Écrire			
InvokeMcp	Autorise l'utilisation du service MCP	List			

Types de ressources définis par le AWS serveur MCP

AWS Le serveur MCP ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au serveur AWS MCP, spécifiez-le `"Resource": "*"` dans votre politique.

Clés de condition pour le AWS serveur MCP

AWS MCP ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Mechanical Turk

Amazon Mechanical Turk (préfixe de service : `mechanicalturk`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Mechanical Turk
- Types de ressources définis par Amazon Mechanical Turk
- Clés de condition pour Amazon Mechanical Turk

Actions définies par Amazon Mechanical Turk

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptQualificationRequest	L' AcceptQualificationRequest opération donne suite à la demande de qualification d'un travailleur	Écrire			
ApproveAssignment	L' ApproveAssignment opération approuve les résultats d'une mission terminée	Écrire			
AssociateQualificationWithWorker	L' AssociateQualificationWithWorker opération donne à un travailleur une qualification	Écrire			
CreateAdditionalAssignmentsForHIT	L'opération CreateAdditionalAssignmentsForHIT augmente le nombre maximum d'assignations d'un HIT existant	Écrire			
CreateHIT	L'opération CreateHIT crée une nouvelle tâche HIT (Human Intelligence Task)	Écrire			
CreateHITType	L'HITType opération Create crée un nouveau type HIT	Écrire			
CreateHITWithHITType	L'HITWithHITType opération Create crée une nouvelle Human Intelligence Task (HIT) à l'aide d'un identifiant	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	HITType existant généré par l'HITType opération Create				
CreateQualificationType	L' CreateQualificationType opération crée un nouveau type de qualification, représenté par une structure QualificationType de données	Écrire			
CreateWorkerBlock	L' CreateWorkerBlock opération vous permet d'empêcher un travailleur de travailler sur votre HITs	Écrire			
DeleteHIT	L'opération DeleteHIT supprime une tâche HIT qui n'est plus nécessaire	Écrire			
DeleteQualificationType	Le DeleteQualificationType supprime un type de qualification et élimine tous les types HIT associés au type de qualification	Écrire			
DeleteWorkerBlock	L' DeleteWorkerBlock opération vous permet de réintégrer un travailleur bloqué pour qu'il travaille sur votre HITs	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateQualificationFromWorker	Le DisassociateQualificationFromWorker révoque une qualification précédemment accordée à un utilisateur	Écrire			
GetAccountBalance	L' GetAccountBalance opération permet de récupérer le montant d'argent sur votre compte Amazon Mechanical Turk	Lecture			
GetAssignment	GetAssignment récupère une affectation dont la AssignmentStatus valeur est Soumise, Approuvée ou Rejetée, en utilisant l'ID de l'affectation	Lecture			
GetFileUploadURL	L'opération GetFileUpload URL génère et renvoie une URL temporaire	Lecture			
GetHIT	L'opération GetHIT récupère les détails de la tâche HIT spécifiée	Lecture			
GetQualificationScore	L' GetQualificationScore opération renvoie la valeur de la qualification d'un travailleur pour un type de qualification donné	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQualificationType	L' GetQualificationType opération récupère des informations sur un type de qualification à l'aide de son identifiant	Lecture			
ListAssignmentsForHIT	L'opération ListAssignmentsFor HIT récupère les tâches terminées pour un HIT	List			
ListBonusPayments	L' ListBonusPayments opération permet de récupérer les montants des bonus que vous avez payés aux travailleurs pour un HIT ou une mission donnée	List			
ListHITs	L'HITs opération List renvoie tous les HITs	List			
ListHITsForQualificationType	L'HITsForQualificationType opération List renvoie les données HITs qui utilisent la valeur donnée Qualifific ationType pour un Qualifica tionRequirement	List			
ListQualificationRequests	L' ListQualificationRequests opération récupère les demandes de qualifications d'un type de qualification particulier	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListQualificationTypes	L' ListQualificationTypes opération recherche les types de qualification à l'aide de la requête de recherche spécifiée et renvoie une liste des types de qualification	List			
ListReviewPolicyResultsForHIT	L'opération ListReviewPolicyResultsFor HIT récupère les résultats calculés et les actions entreprises lors de l'exécution de vos politiques de révision lors d'une opération CreateHit.	List			
ListReviewableHITs	L' ListReviewableHITs opération renvoie tous les demandeurs HITs qui n'ont pas été approuvés ou rejetés	List			
ListWorkerBlocks	L' ListWorkersBlocks opération permet de récupérer une liste des travailleurs empêchés de travailler sur votre HITs	List			
ListWorkersWithQualificationType	L' ListWorkersWithQualificationType opération renvoie tous les travailleurs avec un type de qualification donné	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
NotifyWorkers	L' NotifyWorkers opération envoie un e-mail à un ou plusieurs travailleurs que vous spécifiez à l'aide de l'identifiant du travailleur	Écrire			
RejectAssignment	L' RejectAssignment opération rejette les résultats d'une mission terminée	Écrire			
RejectQualificationRequest	L' RejectQualificationRequest opération rejette la demande de qualification d'un utilisateur	Écrire			
SendBonus	L' SendBonus opération émet un paiement d'argent de votre compte à un travailleur	Écrire			
SendTestEventNotification	L' SendTestEventNotification opération amène Amazon Mechanical Turk à envoyer un message de notification comme si un événement HIT s'était produit, conformément à la spécification de notification fournie	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateExpirationForHIT	L'opération UpdateExpirationFor HIT vous permet de prolonger le délai d'expiration d'un HIT au-delà de son expiration actuelle ou de faire expirer un HIT immédiatement	Écrire			
UpdateHITReviewStatus	L'opération Update HITReviewStatus change le statut d'un HIT	Écrire			
UpdateHITTypeOfHIT	L'opération Update HITTypeofHIT permet de modifier les HITType propriétés d'un HIT	Écrire			
UpdateNotificationSettings	L' UpdateNotificationSettings opération crée, met à jour, désactive ou réactive les notifications pour un type HIT	Écrire			
UpdateQualificationType	L' UpdateQualificationType opération modifie les attributs d'un type de qualification existant, qui est représenté par une structure de QualificationType données	Écrire			

Types de ressources définis par Amazon Mechanical Turk

Amazon Mechanical Turk ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à Amazon Mechanical Turk, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Amazon Mechanical Turk

MechanicalTurk ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon MemoryDB

Amazon MemoryDB (préfixe de service : `memorydb`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon MemoryDB
- Types de ressources définis par Amazon MemoryDB
- Clés de condition pour Amazon MemoryDB

Actions définies par Amazon MemoryDB

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> Lorsque vous créez une politique MemoryDB for Redis dans IAM, vous devez utiliser le caractère générique « * » pour le bloc Resource (Ressource). Pour de plus amples d'informations sur l'utilisation des actions d'API MemoryDB for Redis suivantes dans une politique IAM, consultez Actions MemoryDB et IAM.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdateCluster	Accorde l'autorisation d'appliquer les mises à jour de service	Écrire	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
Connect	Autorise un utilisateur ou un rôle IAM à se connecter en tant qu'utilisateur spécifié MemoryDB à un nœud d'un cluster	Écrire	cluster*		
			user*		
				aws:ResourceTag/${TagKey}	
CopySnapshot	Accorde l'autorisation de créer une copie d'un instantané existant	Écrire	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	Accorde l'autorisation de créer une liste de contrôle d'accès	Écrire	user*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCluster	Accorde l'autorisation de créer un cluster	Écrire	acl*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
			parametergroup*		
			subnetgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateMultiRegionCluster	Accorde les autorisations nécessaires à la création d'un cluster multirégional	Écrire	multiregionparametergroup*		memorydb:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydb:TLSEnabled	
CreateParameterGroup	Accorde l'autorisation de créer un groupe de paramètres	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSnapshot	Accorde l'autorisation de créer la sauvegarde d'un cluster au moment actuel	Écrire	cluster*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubnetGroup	Accorde l'autorisation de créer un groupe de sous-réseaux	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUser	Accorde l'autorisation de créer un utilisateur	Écrire		aws:RequestTag/${TagKey} aws:TagKeys memorydb:UserAuthenticationMode	memorydb:TagResource
DeleteAcl	Accorde l'autorisation de supprimer une liste de contrôle d'accès	Écrire	acl*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCluster	Accorde l'autorisation de supprimer un cluster précédemment approvisionné	Écrire	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey}	
DeleteMultiRegionCluster	Accorde les autorisations nécessaires pour supprimer un cluster multirégional	Écrire	multiregioncluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteParameterGroup	Accorde l'autorisation de supprimer un groupe de paramètres	Écrire	parametergroup*		
				aws:ResourceTag/${TagKey}	
DeleteSnapshot	Accorde l'autorisation de supprimer un instantané	Écrire	snapshot*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSubnetGroup	Accorde l'autorisation de supprimer un groupe de sous-réseaux	Écrire	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteUser	Accorde l'autorisation de supprimer un utilisateur	Écrire	user*		
				aws:ResourceTag/${TagKey}	
DescribeAcls	Accorde l'autorisation de récupérer des informations sur les listes de contrôle d'accès.	Lecture	acl*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DescribeClusters	Accorde l'autorisation de récupérer des informations sur tous les clusters approvisionnés si aucun identifiant de cluster n'est spécifié, ou sur un cluster spécifique si un identifiant de cluster est fourni	Lecture	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeEngineVersions	Accorde l'autorisation de répertorier les moteurs disponibles et leurs versions	Lecture			
DescribeEvents	Accorde l'autorisation de récupérer les événements liés aux clusters, aux groupes de sécurité de cache et aux groupes de paramètres	Lecture			
DescribeMultiRegionClusters	Accorde les autorisations nécessaires pour récupérer des informations sur tous les clusters multirégionaux si aucun identifiant de cluster n'est spécifié, ou sur un cluster multirégional spécifique si un identifiant de cluster est fourni	Lecture	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeMultiRegionParameterGroups	Accorde les autorisations nécessaires pour récupérer des informations sur les groupes de paramètres multirégionaux	Lecture	multiregionparametergroup*		
DescribeMultiRegionParameters	Accorde les autorisations nécessaires pour récupérer une liste de paramètres détaillée pour un groupe de paramètres multi-régions particulier	Lecture	multiregionparametergroup*		
DescribeParameterGroups	Accorde l'autorisation de récupérer des informations sur les groupes des paramètres	Lecture	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeParameters	Accorde l'autorisation de renvoyer une liste détaillée des paramètres pour un groupe de paramètres particulier	Lecture	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodes	Accorde des autorisations de récupérer des nœuds réservés	Lecture	reservednode*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DescribeReservedNodesOfferings	Accorde des autorisations pour récupérer des offres de nœuds réservés	Lecture			
DescribeServiceUpdates	Accorde l'autorisation de récupérer les détails des mises à jour du service	Lecture			
DescribeSnapshots	Accorde l'autorisation de récupérer les informations sur les instantanés de cluster	Lecture	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeSubnetGroups	Accorde l'autorisation de récupérer une liste des groupes de sous-réseaux	Lecture	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Accorde l'autorisation de récupérer les informations sur les utilisateurs	Lecture	user*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
FailoverShard	Accorde l'autorisation de tester le basculement automatique sur une partition spécifiée dans un cluster	Écrire	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
ListAllowedMultiRegionClusterUpdates	Accorde les autorisations nécessaires pour répertorier les mises à jour de clusters multirégionaux disponibles	Lecture	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAllowedNodeTypeUpdates	Accorde l'autorisation de répertorier les mises à jour des types de nœud disponibles	Lecture	cluster*		
				aws:ResourceTag/${TagKey}	
ListTags	Accorde l'autorisation de répertorier les balises d'une allocation des coûts	Lecture	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:ResourceTag/${TagKey}	
PauseMultiRegionClusterReplication [autorisation uniquement]	Accorde l'autorisation de suspendre la réplication pour un cluster multirégional	Écrire	multiregioncluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
PurchaseReservedNodesOffering	Accorde l'autorisation d'acheter un nouveau nœud réservé	Écrire	reservednode*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ResetParameterGroup	Accorde l'autorisation de modifier les paramètres d'un groupe de paramètres par la valeur par défaut du moteur ou du système	Écrire	parametergroup*		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation d'ajouter jusqu'à 10 balises d'allocation des coûts à la ressource nommée	Identification	acl		
			cluster		
			multiregioncluster		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			parameter group		
			reservednode		
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde les autorisations nécessaires pour supprimer les balises identifiées par la TagKeys liste d'une ressource	Identification	acl		
			cluster		
			multiregioncluster		
			parameter group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAcl	Accorde l'autorisation de mettre à jour une liste de contrôle d'accès	Écrire	acl*		
			user*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCluster	Accorde l'autorisation de mettre à jour les paramètres d'un cluster	Écrire	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			acl		
			parameter group		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMultiRegionCluster	Accorde les autorisations nécessaires pour mettre à jour les paramètres d'un cluster multirégional	Écrire	multiregioncluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregionparametergroup		
				aws:ResourceTag/${TagKey}	
UpdateParameterGroup	Accorde l'autorisation de mettre à jour les paramètres dans un groupe de paramètres	Écrire	parametergroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateSubnetGroup	Accorde l'autorisation de mettre à jour un groupe de sous-réseaux	Écrire	subnetgroup*		
				aws:ResourceTag/${TagKey}	
UpdateUser	Accorde l'autorisation de mettre à jour un utilisateur	Écrire	user*		
				aws:ResourceTag/${TagKey} memorydb:UserAuthenticationMode	

Types de ressources définis par Amazon MemoryDB

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> Le nom de la ressource dans la chaîne ARN doit être en minuscules pour être effectif.

Types de ressources	ARN	Clés de condition
multiregionparametergroup	`arn:${Partition}:memorydb::${Account}:multiregionparametergroup/${MultiRegionParameterGroupName}`	
parametergroup	`arn:${Partition}:memorydb:${Region}:${Account}:parametergroup/${ParameterGroupName}`	aws:ResourceTag/${TagKey}
subnetgroup	`arn:${Partition}:memorydb:${Region}:${Account}:subnetgroup/${SubnetGroupName}`	aws:ResourceTag/${TagKey}
multiregioncluster	`arn:${Partition}:memorydb::${Account}:multiregioncluster/${ClusterName}`	aws:ResourceTag/${TagKey} memorydb:TLSEnabled
cluster	`arn:${Partition}:memorydb:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:memorydb:${Region}:${Account}:snapshot/${SnapshotName}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:memorydb:${Region}:${Account}:user/${UserName}`	aws:ResourceTag/${TagKey}
acl	`arn:${Partition}:memorydb:${Region}:${Account}:acl/${AclName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
reservednode	`arn:${Partition}:memorydb:${Region}:${Account}:reservednode/${ReservationID}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon MemoryDB

Amazon MemoryDB définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction des balises qui sont transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des balises associées à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction des clés de balise qui sont transmises dans la demande	ArrayOfString
memorydb:TLSEnabled	Filtre l'accès en fonction du TLSEnabled paramètre présent dans la demande ou utilise par défaut la valeur vraie si le paramètre n'est pas présent	Booléen
memorydb:UserAuthenticationMode	Filtre l'accès par le paramètre UserAuthentication Mode .Type dans la requête	String

Actions, ressources et clés de condition pour Amazon Message Delivery Service

Amazon Message Delivery Service (préfixe de service : `ec2messages`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Message Delivery Service
- Types de ressources définis par Amazon Message Delivery Service
- Clés de condition pour Amazon Message Delivery Service

Actions définies par Amazon Message Delivery Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcknowledgeMessage	Accorde l'autorisation d'accuser réception d'un message, ce qui garantit qu'il ne sera pas de nouveau remis	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteMessage	Accorde l'autorisation de supprimer un message	Écriture			
FailMessage	Accorde l'autorisation de déclarer l'échec d'un message, ce qui signifie que le message n'a pas pu être traité et qu'il ne peut pas faire l'objet d'une réponse ni d'une nouvelle remise	Écriture			
GetEndpoint	Accorde l'autorisation d'acheminer le trafic vers le point de terminaison qui convient en fonction de la destination donnée des messages	Lecture			
GetMessages	Accorde l'autorisation de transmettre des messages à clients/instances l'utilisateur utilisant un long sondage	Lecture		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendReply	Accorde l'autorisation d'envoyer des réponses depuis clients/instances le service en amont	Écrire		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Types de ressources définis par Amazon Message Delivery Service

Amazon Message Delivery Service ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à Amazon Message Delivery Service, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Amazon Message Delivery Service

Amazon Message Delivery Service définit les clés de condition suivantes, que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
ec2:SourceInstanceARN	Filtre l'accès en fonction de l'ARN de l'instance à l'origine de la demande.	ARN
ssm:SourceInstanceARN	Filtre l'accès en vérifiant le nom de ressource Amazon (ARN) de l'instance gérée par le responsable des AWS systèmes à partir de laquelle la demande est faite. Cette	ARN

Clés de condition	Description	Type
	clé n'est pas présente uniquement si la demande provient de l'instance gérée authentifiée avec un rôle IAM associé à un profil d'instance EC2	

Actions, ressources et clés de condition pour Amazon Message Gateway Service

Amazon Message Gateway Service (préfixe de service :`ssmmessages`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Message Gateway Service
- Types de ressources définis par Amazon Message Gateway Service
- Clés de condition pour Amazon Message Gateway Service

Actions définies par Amazon Message Gateway Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateControlChannel	Accorde l'autorisation d'enregistrer un canal de contrôle pour qu'une instance envoie des messages de contrôle au service Systems Manager	Écriture		ssm:SourceInstanceARN ec2:SourceInstanceARN	
CreateDataChannel	Accorde l'autorisation d'enregistrer un canal de données pour qu'une instance envoie des messages de données au service Systems Manager	Écriture			
OpenControlChannel	Accorde l'autorisation d'ouvrir une connexion WebSocket pour un flux de canal de contrôle enregistré entre une instance et le service Systems Manager	Écriture			
OpenDataChannel	Accorde l'autorisation d'ouvrir une connexion WebSocket pour un flux de canal de données enregistré entre une instance et le service Systems Manager	Écrire			

Types de ressources définis par Amazon Message Gateway Service

Amazon Message Gateway Service ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon Message Gateway Service, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Amazon Message Gateway Service

Amazon Message Gateway Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
ec2:SourceInstanceARN	Filtre l'accès en fonction de l'ARN de l'instance à l'origine de la demande.	ARN
ssm:SourceInstanceARN	Filtre l'accès en vérifiant le nom de ressource Amazon (ARN) de l'instance gérée par le responsable des AWS systèmes à partir de laquelle la demande est faite. Cette clé n'est pas présente uniquement si la demande provient de l'instance gérée authentifiée avec un rôle IAM associé à un profil d'instance EC2	ARN

Actions, ressources et clés de condition pour AWS Microservice Extractor pour .NET

AWS Microservice Extractor pour .NET (préfixe de service :`serviceextract`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Microservice Extractor pour .NET
- Types de ressources définis par AWS Microservice Extractor pour .NET
- Clés de condition pour AWS Microservice Extractor pour .NET

Actions définies par AWS Microservice Extractor pour .NET

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConfig [autorisation uniquement]	Accorde l'autorisation d'obtenir la configuration requise pour le client de AWS bureau Microservice Extractor pour .NET	Lecture			

Types de ressources définis par AWS Microservice Extractor pour .NET

AWS Microservice Extractor pour .NET ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Microservice Extractor for .NET, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Microservice Extractor pour .NET

Microservice Extractor for .NET ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les crédits du programme AWS Migration Acceleration

AWS Migration Acceleration Program Credits (préfixe de service :`mapcredits`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les crédits du programme AWS Migration Acceleration
- Types de ressources définis par les crédits du AWS Migration Acceleration Program
- Clés de condition pour les crédits du programme AWS Migration Acceleration

Actions définies par les crédits du programme AWS Migration Acceleration

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAssociatedPrograms [autorisation uniquement]	Accorde l'autorisation de consulter les accords du programme d'accélération de la migration associés à l'utilisateur	List	agreement*		
ListQuarterCredits [autorisation uniquement]	Accorde l'autorisation de consulter les crédits d'accords du programme d'accélération de la migration associés au compte payeur de l'utilisateur	List	agreement*		
ListQuarterSpend [autorisation uniquement]	Accorde l'autorisation de consulter les dépenses éligibles aux accords du programme d'accélération de la migration associées au compte payeur de l'utilisateur	List	agreement*		

Types de ressources définis par les crédits du AWS Migration Acceleration Program

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
agreement	`arn:${Partition}:mapcredits:::${Agreement}/${AgreementId}`	

Clés de condition pour les crédits du programme AWS Migration Acceleration

MapCredits ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Migration Hub

AWS Migration Hub (préfixe de service :`mgh`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Migration Hub
- Types de ressources définis par AWS Migration Hub
- Clés de condition pour AWS Migration Hub

Actions définies par AWS Migration Hub

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptConnection	Accorde l'autorisation d'accepter une connexion	Écrire	ConnectionResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
AssociateAutomationUnitRole	Accorde l'autorisation d'associer un rôle IAM à une unité d'automatisation	Écrire	AutomationUnitResource*		
AssociateCreatedArtifact	Permet d'associer un AWS artefact donné à un Migration Task	Écrire	migrationTask*		
AssociateDiscoveredResource	Accorde l'autorisation d'associer une ressource ADS donnée à un MigrationTask	Écrire	migrationTask*		
AssociateSourceResource	Accorde l'autorisation d'associer une ressource source	Écrire	migrationTask*		
BatchAssociateIamRoleWithConnection	Accorde l'autorisation d'associer par lots des rôles IAM à une connexion	Écrire	ConnectionResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDisassociateIamRoleFromConnection	Accorde l'autorisation de dissocier par lots les rôles IAM d'une connexion	Écrire	ConnectionResource*		
CreateAutomationRun	Accorde l'autorisation de créer une unité d'automatisation exécutée	Écrire			
CreateAutomationUnit	Autorise la création d'une unité d'automatisation	Écrire			
CreateHomeRegionControl	Accorde l'autorisation de créer un contrôle de la région d'origine du Migration Hub	Écrire			
CreateProgressUpdateStream	Accorde l'autorisation de créer un ProgressUpdateStream	Écrire	progressUpdateStream*		
DeleteAutomationRun	Autorise la suppression d'une unité d'automatisation exécutée	Écrire	AutomationRunResource*		
DeleteAutomationUnit	Autorise la suppression d'une unité d'automatisation	Écrire	AutomationUnitResource*		
DeleteConnection	Accorde l'autorisation de supprimer une connexion.	Écrire	ConnectionResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteHomeRegionControl	Accorde l'autorisation de supprimer un contrôle de la région d'origine du Migration Hub	Écrire			
DeleteProgressUpdateStream	Accorde l'autorisation de supprimer un ProgressUpdateStream	Écrire	progressUpdateStream*		
DescribeApplicationState	Accorde l'autorisation d'obtenir l'état d'une application Application Discovery Service	Lecture			
DescribeAutomationRun	Accorde l'autorisation de décrire le fonctionnement d'une unité d'automatisation	Lecture	AutomationRunResource*		
DescribeAutomationUnit	Autorise la description d'une unité d'automatisation	Lecture	AutomationUnitResource*		
DescribeHomeRegionControls	Accorde l'autorisation de répertorier les contrôles de la région d'origine	List			
DescribeMigrationTask	Accorde l'autorisation de décrire un MigrationTask	Lecture	migrationTask*		
DisassociateAutomationUnitRole	Accorde l'autorisation de dissocier un rôle IAM d'une unité d'automatisation	Écrire	AutomationUnitResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateCreatedArtifact	Accorde l'autorisation de dissocier un AWS artefact donné d'un MigrationTask	Écrire	migrationTask*		
DisassociateDiscoveredResource	Accorde l'autorisation de dissocier une ressource ADS donnée d'un MigrationTask	Écrire	migrationTask*		
DisassociateSourceResource	Accorde l'autorisation de dissocier la ressource source	Écrire	migrationTask*		
GetConnection	Accorde l'autorisation d'obtenir une connexion	Lecture	ConnectionResource*		
GetHomeRegion	Accorde l'autorisation d'obtenir la région d'origine du Migration Hub	Lecture			
ImportMigrationTask	Autorise l'importation d'un MigrationTask	Écrire	migrationTask*		
ListApplicationStates	Accorde l'autorisation de répertorier les statuts de l'application	List			
ListAutomationRuns	Accorde l'autorisation de répertorier les exécutions des unités d'automatisation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAutomationUnits	Accorde l'autorisation de répertorier les unités d'automatisation	List			
ListConnectionRoles	Accorde l'autorisation de répertorier les rôles de connexion	List	ConnectionResource*		
ListConnections	Accorde l'autorisation de répertorier les connexions	List			
ListCreatedArtifacts	Accorde l'autorisation de répertorier les artefacts créés associés pour un Migration Task	List	migrationTask*		
ListDiscoveredResources	Accorde l'autorisation de répertorier les ressources ADS associées à partir de Migration Task	List	migrationTask*		
ListMigrationTaskUpdates	Accorde l'autorisation de répertorier les mises à jour des tâches de migration	List	migrationTask*		
ListMigrationTasks	Accorde l'autorisation de mettre en vente Migration Tasks	List			
ListProgressUpdateStreams	Accorde l'autorisation de mettre en vente ProgressUpdateStreams	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSourceResources	Accorde l'autorisation de répertorier les ressources sources	List	migrationTask*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource.	List			
NotifyApplicationState	Accorde l'autorisation de mettre à jour l'état d'une application Application Discovery Service.	Écrire			
NotifyMigrationTaskState	Accorde l'autorisation de notifier le dernier Migration Task État	Écrire	migrationTask*		
PutResourceAttributes	Donne l'autorisation de mettre ResourceAttributes	Écrire	migrationTask*		
RejectConnection	Autorise le rejet d'une connexion	Écrire	ConnectionResource*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification		aws:TagKeys	

Types de ressources définis par AWS Migration Hub

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
progressUpdateStream	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}`	
migrationTask	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}/migrationTask/${Task}`	
AutomationRunResource	`arn:${Partition}:mgh:${Region}:${Account}:automation-run/${RunID}`	mgh:AutomationRunResourceRunID
AutomationUnitResource	`arn:${Partition}:mgh:${Region}:${Account}:automation-unit/${AutomationUnitId}`	mgh:AutomationUnitResourceAutomationUnitArn

Types de ressources	ARN	Clés de condition
ConnectionResource	`arn:${Partition}:mgh:${Region}:${Account}:${ConnectionArn}`	aws:ResourceTag/${TagKey} mgh:ConnectionResourceConnectionArn

Clés de condition pour AWS Migration Hub

AWS Migration Hub définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString
mgh:AutomationRunResourceRunID	AutomationRunResource identifiant RunID de ressource	String
mgh:AutomationUnitResourceA	AutomationUnitResource automationUnitArn identifiant de ressource	ARN

Clés de condition	Description	Type
utomation UnitArn		
mgh:Conne ctionReso urceConne ctionArn	ConnectionResource identifiant ConnectionArn de ressource	String

Actions, ressources et clés de condition pour AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator (préfixe de service :`migrationhub-orchestrator`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Migration Hub Orchestrator
- Types de ressources définis par AWS Migration Hub Orchestrator
- Clés de condition pour AWS Migration Hub Orchestrator

Actions définies par AWS Migration Hub Orchestrator

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTemplate	Accorde l'autorisation de créer un modèle personnalisé	Écrire			
CreateWorkflow	Accorde l'autorisation de créer un flux de travail basé sur le modèle sélectionné	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowStep	Accorde l'autorisation de créer une étape sous un flux de travail et un groupe d'étapes spécifique	Écrire	workflow*		
CreateWorkflowStepGroup	Accorde l'autorisation de créer un groupe d'étapes personnalisé pour un flux de travail donné	Écrire	workflow*		
DeleteTemplate	Accorde l'autorisation de supprimer un modèle personnalisé	Écrire	template*		
DeleteWorkflow	Accorde l'autorisation de créer un flux de travail	Écrire	workflow*		
DeleteWorkflowStep	Accorde l'autorisation de supprimer une étape d'un	Écrire	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	groupe d'étapes spécifique dans un flux de travail				
DeleteWorkflowStepGroup	Accorde l'autorisation de supprimer un groupe d'étapes associé à un flux de travail	Écrire	workflow*		
GetMessage	Accorde l'autorisation au plugin de recevoir des informations du service	Lecture			
GetTemplate	Accorde l'autorisation d'obtenir des métadonnées depuis un modèle	Lecture	template*		
GetTemplateStep	Accorde l'autorisation de récupérer les détails d'une étape associée à un modèle et à un groupe d'étapes	Lecture	template*		
GetTemplateStepGroup	Accorde l'autorisation de récupérer les métadonnées d'un groupe d'étapes sous un modèle	Lecture	template*		
GetWorkflow	Accorde l'autorisation de récupérer les métadonnées associées à un flux de travail	Lecture	workflow*		
GetWorkflowStep	Accorde l'autorisation d'obtenir les détails de l'étape associée à un flux de travail et à un groupe d'étapes	Lecture	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkflowStepGroup	Accorde l'autorisation d'obtenir les détails d'un groupe d'étapes associé à un flux de travail	Lecture	workflow*		
ListPlugins	Accorde l'autorisation d'obtenir une liste de tous les plugins enregistrés	List			
ListTagsForResource	Accorde l'autorisation d'obtenir une liste d'identifications pour la ressource spécifiée	Lecture	template* workflow*		
ListTemplateStepGroups	Accorde l'autorisation de répertorier les groupes d'étapes d'un modèle	List	template*		
ListTemplateSteps	Accorde l'autorisation d'obtenir une liste d'étapes dans un groupe d'étapes	List	template*		
ListTemplates	Accorde l'autorisation d'obtenir une liste de tous les modèles disponibles pour le client	List			
ListWorkflowStepGroups	Accorde l'autorisation d'obtenir une liste des groupes d'étapes associés à un flux de travail	List	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWorkflowSteps	Accorde l'autorisation d'obtenir une liste d'étapes dans un groupe d'étapes associé à un flux de travail	List	workflow*		
ListWorkflows	Accorde l'autorisation de répertorier tous les flux de travail	List			
RegisterPlugin	Accorde l'autorisation d'enregistrer le plugin pour recevoir un ID et commencer à recevoir des messages du service	Écrire			
RetryWorkflowStep	Accorde l'autorisation de réessayer l'exécution d'une étape échouée dans un flux de travail	Écrire	workflow*		
SendMessage	Accorde l'autorisation au plugin d'envoyer des informations au service	Écrire			
StartWorkflow	Accorde l'autorisation de démarrer un flux de travail ou de reprendre un flux de travail arrêté	Écrire	workflow*		
StopWorkflow	Accorde l'autorisation d'arrêter un flux de travail	Écrire	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	template		
			workflow		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	template		
			workflow		
				aws:TagKeys	
UpdateTemplate	Autorise la mise à jour d'un modèle personnalisé	Écrire	template*		
UpdateWorkflow	Accorde l'autorisation de mettre à jour des métadonnées associées à un flux de travail	Écrire	workflow*		
UpdateWorkflowStep	Accorde l'autorisation de mettre à jour les métadonnées et l'état d'une étape personnalisée dans un flux de travail	Écrire	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateWorkflowStepGroup	Accorde l'autorisation de mettre à jour les métadonnées associées à un groupe d'étapes dans un flux de travail donné	Écrire	workflow*		

Types de ressources définis par AWS Migration Hub Orchestrator

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workflow	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:workflow/${ResourceId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:template/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les

conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces (préfixe de service :`refactor-spaces`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Migration Hub Refactor Spaces
- Types de ressources définis par AWS Migration Hub Refactor Spaces
- Clés de condition pour les espaces de refactorisation du AWS Migration Hub

Actions définies par AWS Migration Hub Refactor Spaces

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApplication	Accorde l'autorisation de créer une application dans un environnement	Écrire		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Accorde l'autorisation de créer un environnement	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRoute	Accorde l'autorisation de créer un routage dans une application	Écrire		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateService	Accorde l'autorisation de créer un service dans une application	Écrire		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Accorde l'autorisation de supprimer une application d'un environnement	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
DeleteEnvironment	Accorde l'autorisation de supprimer un environnement	Écrire	environment*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource	Écrire			
DeleteRoute	Accorde l'autorisation de supprimer un routage d'une application	Écrire	route*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteService	Accorde l'autorisation de supprimer un service d'une application	Écrire	service*		
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetApplication	Accorde l'autorisation d'obtenir plus d'informations sur une application	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetEnvironment	Accorde l'autorisation d'obtenir plus d'informations pour un environnement	Lecture	environment*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Accorde l'autorisation d'obtenir les informations sur une politique de ressource	Lecture			
GetRoute	Accorde l'autorisation d'obtenir plus d'informations sur un routage	Lecture	route*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetService	Accorde l'autorisation d'obtenir plus d'informations sur un service	Lecture	service*		
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
ListApplications	Accorde l'autorisation de répertorier toutes les applications d'un environnement	Lecture	application*		
ListEnvironmentVpcs	Accorde l'autorisation de tout répertorier VPCs pour l'environnement	Lecture	environment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEnvironments	Accorde l'autorisation de répertorier tous les environnements	Lecture			
ListRoutes	Accorde l'autorisation de répertorier tous les routages d'une application	Lecture	route*		
ListServices	Accorde l'autorisation de répertorier tous les services d'un environnement	Lecture	environment*		
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises d'une ressource donnée	Lecture			
PutResourcePolicy	Accorde l'autorisation d'ajouter une politique de ressource	Écrire			
TagResource	Accorde l'autorisation de baliser une ressource	Identification	application		
			environment		
			route		
			service		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	application		
			environment		
			route		
			service		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdateRoute	Accorde l'autorisation de mettre à jour un routage d'une application	Écrire	route*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS Migration Hub Refactor Spaces

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
environment	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds
service	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/service/${ServiceId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:ServiceCreatedByAccount

Types de ressources	ARN	Clés de condition
route	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/route/${RouteId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:RouteCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:SourcePath

Clés de condition pour les espaces de refactorisation du AWS Migration Hub

AWS Migration Hub Refactor Spaces définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
refactor-spaces:ApplicationCreatedByAccount	Filtre l'accès en limitant l'action uniquement aux comptes qui ont créé l'application dans un environnement	String
refactor-spaces:CreatedByAccountIds	Filtre l'accès en fonction des comptes qui ont créé la ressource	ArrayOfString
refactor-spaces:RouteCreatedByAccount	Filtre l'accès en limitant l'action uniquement aux comptes qui ont créé le routage dans une application	String
refactor-spaces:ServiceCreatedByAccount	Filtre l'accès en limitant l'action uniquement aux comptes qui ont créé le service dans une application	String
refactor-spaces:SourcePath	Filtre l'accès en fonction du chemin du routage	String

Actions, ressources et clés de condition pour les recommandations stratégiques du AWS Migration Hub

AWS Les recommandations de stratégie du Migration Hub (préfixe de service :`migrationhub-strategy`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les recommandations de la stratégie du AWS Migration Hub
- Types de ressources définis par les recommandations de la stratégie de AWS Migration Hub
- Clés de condition pour les recommandations de stratégie de AWS Migration Hub

Actions définies par les recommandations de la stratégie du AWS Migration Hub

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAntiPattern	Accorde l'autorisation d'obtenir des détails sur chaque anti-motif que le collecteur doit examiner dans l'environnement d'un client	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetApplicationComponentDetails	Accorde l'autorisation d'obtenir les détails d'une application	Lecture			
GetApplicationComponentStrategies	Accorde l'autorisation d'obtenir une liste de l'ensemble des politiques et outils recommandés pour une application en cours d'exécution sur un serveur	Lecture			
GetAssessment	Accorde l'autorisation de récupérer le statut d'une évaluation continue	Lecture			
GetImportFileTask	Accorde l'autorisation d'obtenir les détails d'une tâche d'importation spécifique	Lecture			
GetLatestAssessmentId	Accorde l'autorisation de récupérer le dernier identifiant d'évaluation	Lecture			
GetMessage	Autorise le collecteur à recevoir des informations du service	Lecture			
GetPortfolioPreferences	Accorde l'autorisation de récupérer les migration/ Modernization préférences du client	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPortfolioSummary	Accorde l'autorisation de récupérer le résumé global (nombre de serveurs à réhéberger, etc. ainsi que le nombre global d'anti-modèles)	Lecture			
GetRecommendationReportDetails	Accorde l'autorisation de récupérer des informations détaillées sur un rapport de recommandation	Lecture			
GetServerDetails	Accorde l'autorisation d'obtenir des informations sur un serveur spécifique	Lecture			
GetServerStrategies	Accorde l'autorisation d'obtenir les politiques et outils recommandés pour un serveur spécifique	Lecture			
ListAnalyzableServers	Accorde l'autorisation d'obtenir une liste de tous les serveurs analysables dans l'environnement vcenter d'un client	List			
ListAntiPatterns	Accorde l'autorisation d'obtenir une liste des tous les anti-modèles que le collecteur doit rechercher dans l'environnement d'un client	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplicationComponents	Accorde l'autorisation d'obtenir une liste de toutes les applications en cours d'exécution sur les serveurs du client	List			
ListCollectors	Accorde l'autorisation d'obtenir une liste de tous les collecteurs installés par le client	List			
ListImportFileTask	Accorde l'autorisation d'obtenir la liste de toutes les importations effectuées par le client	List			
ListJarArtifacts	Accorde l'autorisation d'obtenir une liste de binaires que le collecteur doit évaluer	List			
ListServers	Accorde l'autorisation d'obtenir une liste de tous les serveurs dans l'environnement d'un client	List			
PutLogData	Autorise le collecteur à envoyer des journaux au service	Écrire			
PutMetricData	Autorise le collecteur à envoyer des métriques au service	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutPortfolioPreferences	Accorde l'autorisation d'enregistrer les Migration/Modernization préférences du client	Écrire			
RegisterCollector	Autorise à enregistrer le collecteur pour recevoir un ID et commencer à recevoir des messages du service	Écrire			
SendMessage	Autorise le collecteur à envoyer des informations au service	Écrire			
StartAssessment	Accorde l'autorisation de démarrer l'évaluation dans l'environnement d'un client (collecte des données de tous les serveurs et fournir des recommandations)	Écrire			
StartImportFileTask	Accorde l'autorisation de commencer à importer des données à partir d'un fichier fourni par le client	Écrire			
StartRecommendationReportGeneration	Accorde l'autorisation de commencer la génération d'un rapport de recommandations	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopAssessment	Accorde l'autorisation d'arrêter une évaluation en cours	Écrire			
UpdateApplicationComponentConfig	Accorde l'autorisation de mettre à jour les détails d'une application	Écrire			
UpdateCollectorConfiguration	Accorde l'autorisation au collecteur d'envoyer des informations au service	Écrire			
UpdateServerConfig	Autorise à mettre à jour les informations sur un serveur en même temps que la stratégie recommandée	Écrire			

Types de ressources définis par les recommandations de la stratégie de AWS Migration Hub

AWS Les recommandations de stratégie du Migration Hub ne prennent pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser à accéder à AWS Migration Hub Strategy Recommendations, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour les recommandations de stratégie de AWS Migration Hub

Migration Hub Strategy Recommendations ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Mobile Analytics

Amazon Mobile Analytics (préfixe de service : `mobileanalytics`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Mobile Analytics
- Types de ressources définis par Amazon Mobile Analytics
- Clés de condition pour Amazon Mobile Analytics

Actions définies par Amazon Mobile Analytics

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFinancialReports	Accorder l'accès aux métriques financières d'une application	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetReports	Accorder l'accès aux métriques standard d'une application	Lecture			
PutEvents	L' PutEvents opération enregistre un ou plusieurs événements	Écrire			

Types de ressources définis par Amazon Mobile Analytics

Amazon Mobile Analytics ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à Amazon Mobile Analytics, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Amazon Mobile Analytics

Mobile Analytics ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Monitron

Amazon Monitron (préfixe de service : `monitron`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Monitron
- Types de ressources définies par Amazon Monitron
- Clés de condition pour Amazon Monitron

Actions définies par Amazon Monitron

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateProjectAdminUser [autorisation uniquement]	Accorde l'autorisation d'associer un utilisateur au projet en tant qu'administrateur.	Gestion des autorisations	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryA

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ssociations sso:ListProfileAssociations sso:ListProfiles
CreateProject [autorisation uniquement]	Accorde l'autorisation de créer un projet	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole kms:CreateGrant sso:CreateManagedApplicationInstance sso:DeleteManagedApplicationInstance sso:DescribeRegisteredRegions

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateProjectUserAssociation [autorisation uniquement]	Accorde l'autorisation d'associer un utilisateur au projet	Gestion des autorisations	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUserAccessRoleAssociation [autorisation uniquement]	Accorde l'autorisation d'associer un rôle d'accès à l'utilisateur	Gestion des autorisations	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
DeleteProject [autorisation uniquement]	Accorde l'autorisation de supprimer un projet	Écriture	project*		sso:DeleteManagedApplicationInstance

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteProjectUserAssociation [autorisation uniquement]	Accorde l'autorisation de dissocier un utilisateur du projet	Gestion des autorisations	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
DeleteUserAccessRoleAssociation [autorisation uniquement]	Accorde l'autorisation de dissocier un rôle d’accès de l’utilisateur	Gestion des autorisations	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateProjectAdminUser [autorisation uniquement]	Accorde l'autorisation de dissocier un administrateur du projet.	Gestion des autorisations	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
GetProject [autorisation uniquement]	Accorde l'autorisation d'obtenir des informations sur un projet	Lecture	project*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProjectAdminUser [autorisation uniquement]	Accorde l'autorisation de décrire un administrateur associé au projet.	Lecture	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:ListProfileAssociations
ListProjectAdminUsers [autorisation uniquement]	Accorde l'autorisation de répertorier tous les administrateurs associés au projet.	Gestion des autorisations	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProjectUserAssociations [autorisation uniquement]	Accorde l'autorisation de répertorier tous les modèles associés à un projet	List	project*		sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
ListProjects [autorisation uniquement]	Accorde l'autorisation de répertorier tous les projets.	Liste			
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation de répertorier toutes les balises pour une ressource	Lecture	project		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListUserAccessRoleAssociations [autorisation uniquement]	Accorde l'autorisation de répertorier tous les rôles d'accès associés à l'utilisateur	List	project*		
TagResource [autorisation uniquement]	Accorde l'autorisation de baliser une ressource	Balisage	project		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation d'annuler le balisage d'une ressource	Balisage	project		
				aws:TagKeys	
UpdateProject [autorisation uniquement]	Accorde l'autorisation de mettre à jour un projet	Écriture	project*		

Types de ressources définies par Amazon Monitron

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
project	`arn:${Partition}:monitron:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Monitron

Amazon Monitron définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises attachées à une ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon MQ

Amazon MQ (préfixe de service : `mq`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon MQ
- Types de ressources définis par Amazon MQ
- Clés de condition pour Amazon MQ

Actions définies par Amazon MQ

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBroker	Accorde l'autorisation de créer un agent	Écriture		aws:RequestTag/${TagKey}	ec2:CreateNetworkInterface
				aws:TagKeys	ec2:CreateNetworkInterfacePermission

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:CreateSecurityGroup ec2:CreateVpcEndpoint ec2:DescribeInternetGateways ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute iam:CreateServiceLinkedRole route53:AssociateVPCWithHostedZone
CreateConfiguration	Accorde l'autorisation de créer une configuration pour le nom de configuration spécifié. Amazon MQ utilise la configuration par défaut (le type de moteur et la version du moteur)	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReplicaBroker [autorisation uniquement]	Accorde l'autorisation de créer un agent de réplica	Écrire	brokers*		
CreateTags	Accorde l'autorisation de créer des balises	Balisage	brokers		
			configurations		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Accorde l'autorisation de créer un utilisateur ActiveMQ	Écriture	brokers*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBroker	Accorde l'autorisation de supprimer un agent	Écrire	brokers*		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface
DeleteConfiguration	Accorde l'autorisation de supprimer une configuration	Écrire	configurations*		
DeleteTags	Accorde l'autorisation de supprimer des balises	Balisage	brokers		
			configurations		
				aws:TagKeys	
DeleteUser	Accorde l'autorisation de supprimer un utilisateur ActiveMQ	Écriture	brokers*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeBroker	Accorde l'autorisation de renvoyer des informations sur l'agent spécifié	Lecture	brokers*		
DescribeBrokerEngineTypes	Accorde l'autorisation de renvoyer des informations sur les moteurs d'agent	Lecture			
DescribeBrokerInstanceOptions	Accorde l'autorisation de renvoyer des informations sur les options d'instance d'agent.	Lecture			
DescribeConfiguration	Accorde l'autorisation de renvoyer des informations sur la configuration spécifiée	Lecture	configurations*		
DescribeConfigurationRevision	Accorde l'autorisation de renvoyer la révision de configuration spécifiée pour la configuration indiquée	Lecture	configurations*		
DescribeUser	Accorde l'autorisation de renvoyer des informations sur un utilisateur ActiveMQ	Lecture	brokers*		
ListBrokers	Accorde l'autorisation de renvoyer une liste de tous les agents	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConfigurationRevisions	Accorde l'autorisation de renvoyer une liste de toutes les révisions existantes pour la configuration spécifiée	Liste	configurations*		
ListConfigurations	Accorde l'autorisation de renvoyer une liste de toutes les configurations	Liste			
ListTags	Accorde l'autorisation de renvoyer une liste de balises	Liste	brokers		
			configurations		
ListUsers	Accorde l'autorisation de renvoyer une liste de tous les utilisateurs ActiveMQ	List	brokers*		
Promote	Octroie l'autorisation de promouvoir un agent.	Écrire	brokers*		
RebootBroker	Accorde l'autorisation de redémarrer un agent	Écriture	brokers*		
UpdateBroker	Accorde l'autorisation d'ajouter un changement de configuration en attente à un agent	Écrire	brokers*		
UpdateBrokerAccessConfiguration [autorisation uniquement]	Accorde l'autorisation de mettre à jour la configuration d'authentification et d'autorisation du courtier RabbitMQ	Écrire	brokers*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConfiguration	Accorde l'autorisation de mettre à jour la configuration spécifiée	Écriture	configurations*		
UpdateUser	Accorde l'autorisation de mettre à jour des informations pour un utilisateur ActiveMQ	Écriture	brokers*		

Types de ressources définis par Amazon MQ

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
brokers	`arn:${Partition}:mq:${Region}:${Account}:broker:${BrokerName}:${BrokerId}`	aws:ResourceTag/${TagKey}
configurations	`arn:${Partition}:mq:${Region}:${Account}:configuration:${ConfigurationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon MQ

Amazon MQ définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour une approbation multipartite

L'approbation multipartite (préfixe de service :`mpa`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par approbation multipartite
- Types de ressources définis par approbation multipartite
- Clés de condition pour l'approbation multipartite

Actions définies par approbation multipartite

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelSession	Accorde l'autorisation d'annuler une session d'approbation	Écrire	session*		
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
CreateApprovalTeam	Accorde l'autorisation de créer une équipe d'approbation	Écrire	approval-team*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateIdentitySource	Accorde l'autorisation de créer une source d'identité	Écrire	identity-source*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteIdentitySource	Accorde l'autorisation de supprimer une source d'identité	Écrire	identity-source*		
				aws:ResourceTag/${TagKey}	
DeleteInactiveApprovalTeamVersion	Accorde l'autorisation de supprimer une équipe d'approbation inactive	Écrire	approval-team*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer une politique de ressource.	Gestion des autorisations			
GetApprovalTeam	Accorde l'autorisation de récupérer les informations d'une équipe d'approbation	Lecture	approval-team*		
				aws:ResourceTag/${TagKey}	
GetIdentitySource	Accorde l'autorisation de récupérer les détails d'une source d'identité	Lecture	identity-source*		
				aws:ResourceTag/${TagKey}	
GetPolicyVersion	Accorde l'autorisation de récupérer les détails d'une politique	Lecture			
GetResourcePolicy	Accorde l'autorisation de récupérer les détails d'une ressource spécifique	Lecture			
GetSession	Accorde l'autorisation de récupérer les détails d'une session d'approbation	Lecture	session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
ListApprovalTeams	Accorde l'autorisation de répertorier les équipes d'approbation	List			
ListIdentitySources	Accorde l'autorisation de répertorier les sources d'identité	List			
ListPolicies	Accorde l'autorisation de répertorier les politiques	List			
ListPolicyVersions	Accorde l'autorisation de répertorier les versions des politiques	List			
ListResourcePolicies	Accorde l'autorisation de répertorier les politiques pour une ressource	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSessions	Accorde l'autorisation de répertorier les sessions d'approbation	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource.	Liste			
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de créer ou de mettre à jour des politiques pour une ressource	Gestion des autorisations			
StartActiveApprovalTeamDeletion	Autorise une équipe d'approbation active à démarrer le processus de suppression	Écrire	approval-team*		
				aws:ResourceTag/${TagKey}	
StartApprovalTeamBaseline	Accorde l'autorisation de créer une base de référence pour une équipe d'approbation active	Écrire	approval-team*		
				aws:ResourceTag/${TagKey}	
StartSession [autorisation uniquement]	Accorde l'autorisation de démarrer une session d'approbation	Écrire	session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
TagResource	Accorde l'autorisation de baliser une ressource	Balisage		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification		aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApprovalTeam	Accorde l'autorisation de mettre à jour l'équipe d'approbation	Écrire	approval-team*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par approbation multipartite

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
approval-team	`arn:${Partition}:mpa:${Region}:${Account}:approval-team/${ApprovalTeamId}`	aws:ResourceTag/${TagKey}
identity-source	`arn:${Partition}:mpa:${Region}:${Account}:identity-source/${IdentitySourceId}`	aws:ResourceTag/${TagKey}
session	`arn:${Partition}:mpa:${Region}:${Account}:session/${SessionId}`	aws:ResourceTag/${TagKey}

Clés de condition pour l'approbation multipartite

L'approbation multipartite définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
mpa:ProtectedResourceAccount	Filtre l'accès par le compte propriétaire de la ressource cible de l'opération nécessitant une approbation	String
mpa:RequestedOperation	Filtre l'accès en fonction d'une opération demandée qui nécessite l'approbation de l'équipe avant de pouvoir être exécutée	String

Actions, ressources et clés de condition pour AWS MWAA Serverless

AWS MWAA Serverless (préfixe de service :`airflow-serverless`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS MWAA Serverless
- Types de ressources définis par AWS MWAA Serverless
- Clés de condition pour AWS MWAA Serverless

Actions définies par AWS MWAA Serverless

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkflow	Accorde l'autorisation de créer un nouveau flux de travail	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteWorkflow	Accorde l'autorisation de supprimer un flux de travail.	Écrire	Workflow*		
GetTaskInstance	Accorde l'autorisation de récupérer les détails des tâches pour l'exécution d'un flux de travail	Lecture	Workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkflow	Accorde l'autorisation de récupérer les détails d'un flux de travail	Lecture	Workflow*		
GetWorkflowRun	Accorde l'autorisation de récupérer les détails relatifs à l'exécution d'un flux de travail	Lecture	Workflow*		
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée	Lecture	Workflow*		
				aws:ResourceTag/${TagKey}	
ListTaskInstances	Accorde l'autorisation de répertorier les tâches pour l'exécution d'un flux de travail	List	Workflow*		
ListWorkflowRuns	Accorde l'autorisation de répertorier les exécutions d'un flux de travail	List	Workflow*		
ListWorkflowVersions	Accorde l'autorisation de répertorier les versions du flux de travail	List	Workflow*		
ListWorkflows	Accorde l'autorisation de répertorier les flux de travail	List			
StartWorkflowRun	Accorde l'autorisation de démarrer une exécution de flux de travail à la demande pour le flux de travail	Écrire	Workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopWorkflowRun	Accorde l'autorisation d'arrêter l'exécution d'un flux de travail	Écrire	Workflow*		
TagResource	Accorde l'autorisation d'identificationr la ressource spécifiée.	Balisage	Workflow*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage de la ressource spécifiée.	Identification	Workflow*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateWorkflow	Autorise la mise à jour d'un flux de travail existant	Écrire	Workflow*		

Types de ressources définis par AWS MWAA Serverless

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Workflow	`arn:${Partition}:airflow-serverless:${Region}:${Account}:workflow/${WorkflowId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS MWAA Serverless

AWS MWAA Serverless définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès par paires clé-valeur de balise associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString

Actions, ressources et clés de condition pour Amazon Neptune

Amazon Neptune (préfixe de service : `neptune-db`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Neptune
- Types de ressources définis par Amazon Neptune
- Clés de condition pour Amazon Neptune

Actions définies par Amazon Neptune

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelLoaderJob	Accorde l'autorisation d'annuler une tâche de chargement	Écrire	database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelMLDataProcessingJob	Accorde l'autorisation d'annuler une tâche de traitement de données de ML	Écrire	database*		
CancelMLModelTrainingJob	Accorde l'autorisation d'annuler une tâche d'entraînement de modèle de ML	Écrire	database*		
CancelMLModelTransformJob	Accorde l'autorisation d'annuler une tâche de transformation de modèle de ML	Écrire	database*		
CancelQuery	Accorde l'autorisation d'annuler une requête	Écrire	database*		
CreateMLEndpoint	Accorde l'autorisation de créer un point de terminaison de ML.	Écrire	database*		
DeleteDataViaQuery	Autorise l'exécution de la suppression de données via une requête APIs sur la base de données	Écrire	database*		
				neptune-db:QueryLanguage	
DeleteMLEndpoint	Accorde l'autorisation de supprimer un point de terminaison de ML	Écrire	database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteStatistics	Accorde l'autorisation de supprimer toutes les statistiques dans la base de données	Écrire	database*		
GetEngineStatus	Accorde l'autorisation de vérifier le statut du moteur Neptune	Lecture	database*		
GetGraphSummary	Octroie l'autorisation d'obtenir le récapitulatif du graphique à partir de la base de données	Lecture	database*		
GetLoaderJobStatus	Accorde l'autorisation de vérifier le statut d'une tâche de chargement	Lecture	database*		
GetMLDataProcessingJobStatus	Accorde l'autorisation de vérifier le statut d'une tâche de traitement de données de ML	Lecture	database*		
GetMLEndpointStatus	Accorde l'autorisation de vérifier le statut d'un point de terminaison de ML	Lecture	database*		
GetMLModelTrainingJobStatus	Accorde l'autorisation de vérifier le statut d'une tâche d'entraînement de modèle de ML	Lecture	database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMLModelTransformJobStatus	Accorde l'autorisation de vérifier le statut d'une tâche de transformation de modèle de ML	Lecture	database*		
GetQueryStatus	Accorde l'autorisation de vérifier le statut de toutes les requêtes actives	Lecture	database*		
				neptune-db:QueryLanguage	
GetStatisticsStatus	Accorde l'autorisation de vérifier le statut des statistiques de la base de données	Lecture	database*		
GetStreamRecords	Accorde l'autorisation de récupérer les enregistrements de flux à partir de Neptune	Lecture	database*		
				neptune-db:QueryLanguage	
ListLoaderJobs	Accorde l'autorisation de répertorier toutes les tâches de chargement	List	database*		
ListMLDataProcessingJobs	Accorde l'autorisation de répertorier toutes les tâches de traitement de données de ML	List	database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMLEndpoints	Accorde l'autorisation de répertorier tous les points de terminaison de ML	List	database*		
ListMLModelTrainingJobs	Accorde l'autorisation de répertorier toutes les tâches d'entraînement de modèle de ML	List	database*		
ListMLModelTransformJobs	Accorde l'autorisation de répertorier toutes les tâches de transformation de modèle de ML	List	database*		
ManageStatistics	Accorde l'autorisation de gérer les statistiques dans la base de données	Écrire	database*		
ReadDataViaQuery	Autorise l'exécution de données de lecture via une requête APIs sur la base de données	Lecture	database*		
				neptune-db:QueryLanguage	
ResetDatabase	Accorde l'autorisation d'obtenir le jeton nécessaire à la réinitialisation et réinitialise la base de données Neptune	Écrire	database*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartLoaderJob	Accorde l'autorisation de démarrer une tâche de chargement	Écrire	database*		
StartMLDataProcessingJob	Accorde l'autorisation de démarrer une tâche de traitement de données de ML	Écrire	database*		
StartMLModelTrainingJob	Accorde l'autorisation de démarrer une tâche d'entraînement de modèle de ML	Écrire	database*		
StartMLModelTransformJob	Accorde l'autorisation de démarrer une tâche de transformation de modèle de ML	Écrire	database*		
WriteDataViaQuery	Accorde l'autorisation d'exécuter des données d'écriture via une requête APIs sur la base de données	Écrire	database*		
				neptune-db:QueryLanguage	
connect	Accorde l'autorisation à toutes les actions d'accès aux données dans les versions de moteur antérieures à 1.2.0.0	Écrire	database*		

Types de ressources définis par Amazon Neptune

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
database	`arn:${Partition}:neptune-db:${Region}:${Account}:${ClusterResourceId}/*`	

Clés de condition pour Amazon Neptune

Amazon Neptune définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
neptune-db:QueryLanguage	Filtre l'accès par modèle de graphique	String

Actions, ressources et clés de condition pour Amazon Neptune Analytics

Amazon Neptune Analytics (préfixe de service : `neptune-graph`) fournit les ressources, actions et clés de contexte de condition propres au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Neptune Analytics
- Types de ressources définis par Amazon Neptune Analytics
- Clés de condition pour Amazon Neptune Analytics

Actions définies par Amazon Neptune Analytics

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> Toutes les actions IAM, à l'exception de ReadDataViaQuery « », WriteDataViaQuery « » et « DeleteDataViaQuery », ont une opération d'API correspondante

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelExportTask	Autorise l'annulation d'une tâche d'exportation en cours	Écrire	export-task*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CancelImportTask	Octroie l'autorisation d'annuler une tâche d'importation en cours.	Écrire	import-task*		
CancelQuery	Accorde l'autorisation d'annuler une requête	Écrire	graph*		
				aws:ResourceTag/${TagKey}	
CreateGraph	Octroie l'autorisation de créer un graphique.	Écrire	graph*		iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
CreateGraphSnapshot	Octroie l'autorisation de créer un instantané à partir d'un graphique existant.	Écrire	graph*		
			graph-snapshot*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateGraphUsingImportTask	Octroie l'autorisation de créer un graphique lors de l'importation de données dans le nouveau graphique.	Écrire	graph*		iam:CreateServiceLinkedRole iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey
			import-task*		
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePrivateGraphEndpoint	Octroie l'autorisation de créer un point de terminaison de graphique privé pour accéder au graphique à partir d'un VPC.	Écrire	graph*		ec2:CreateVpcEndpoint ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					route53:AssociateVPCWithHostedZone
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteDataViaQuery	Accorde l'autorisation de supprimer des données via une requête APIs sur le graphique	Écrire	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraph	Octroie l'autorisation de supprimer un graphique.	Écrire	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraphSnapshot	Octroie l'autorisation de supprimer un instantané.	Écrire	graph-snapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePrivateGraphEndpoint	Octroie l'autorisation de supprimer un point de terminaison de graphique privé d'un graphique.	Écrire	graph*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					route53:DisassociateVPCFromHostedZone
				aws:ResourceTag/${TagKey}	
GetEngineStatus	Octroie l'autorisation d'obtenir le statut du moteur du graphique.	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
GetExportTask	Accorde l'autorisation d'obtenir des informations sur une tâche d'exportation	Lecture	export-task*		
				aws:ResourceTag/${TagKey}	
GetGraph	Octroie l'autorisation d'obtenir des détails sur un graphique.	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
GetGraphSnapshot	Octroie l'autorisation d'obtenir des détails sur un instantané.	Lecture	graph-snapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetGraphSummary	Octroie l'autorisation d'obtenir le récapitulatif des données du graphique.	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
GetImportTask	Octroie l'autorisation d'obtenir des informations sur une tâche d'importation.	Lecture	import-task*		
GetPrivateGraphEndpoint	Octroie l'autorisation d'obtenir des informations sur un point de terminaison de graphique privé d'un graphique.	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
GetQueryStatus	Octroie l'autorisation de vérifier le statut d'une requête donnée.	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
GetStatisticsStatus	Octroie l'autorisation d'obtenir les statistiques des données du graphique.	Lecture	graph*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListExportTasks	Accorde l'autorisation de répertorier les tâches d'exportation dans votre compte	Lecture	export-task*		
ListGraphSnapshots	Octroie l'autorisation de répertorier les instantanés de votre compte.	Lecture	graph-snapshot*		
ListGraphs	Octroie l'autorisation de répertorier les graphiques de votre compte.	Lecture	graph*		
ListImportTasks	Octroie l'autorisation de répertorier les tâches d'importation de votre compte.	Lecture	import-task*		
ListPrivateGraphEndpoints	Octroie l'autorisation de répertorier les points de terminaison de graphique privés d'un graphique donné.	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
ListQueries	Accorde l'autorisation de vérifier le statut de toutes les requêtes actives	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Octroie l'autorisation de répertorier les balises d'une ressource Neptune Analytics.	Lecture	graph		
			graph-snapshot		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ReadDataViaQuery	Autorise la lecture des données via une requête APIs sur le graphique	Lecture	graph*		
				aws:ResourceTag/${TagKey}	
ResetGraph	Octroie l'autorisation de réinitialiser un graphique, ce qui supprime toutes les données du graphique.	Écrire	graph*		
				aws:ResourceTag/${TagKey}	
RestoreGraphFromSnapshot	Octroie l'autorisation de créer un graphique à partir d'un instantané existant.	Écrire	graph*		kms:CreateGrant kms:Decrypt kms:DescribeKey
			graph-snapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
StartExportTask	Autorise l'exportation de données à partir d'un graphique existant	Écrire	export-task*		iam:PassRole
			graph*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartGraph	Accorde l'autorisation de démarrer un graphique	Écrire	graph*		kms:Decrypt kms:DescribeKey
				aws:ResourceTag/${TagKey}	
StartImportTask	Autorise l'importation de données dans un graphique existant	Écrire	graph*		iam:PassRole
			import-task*		
StopGraph	Autorise l'arrêt d'un graphique	Écrire	graph*		
				aws:ResourceTag/${TagKey}	
TagResource	Octroie l'autorisation de baliser une ressource Neptune Analytics.	Identification	graph		
			graph-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Octroie l'autorisation de supprimer les balises d'une ressource Neptune Analytics.	Identification	graph		
			graph-snapshot		
				aws:TagKeys	
UpdateGraph	Octroie l'autorisation de modifier un graphique.	Écrire	graph*		
				aws:ResourceTag/${TagKey} neptune-graph:PublicConnectivity	
WriteDataViaQuery	Accorde l'autorisation d'écrire des données via une requête APIs sur le graphe	Écrire	graph*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon Neptune Analytics

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
graph	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph/${ResourceId}`	aws:ResourceTag/${TagKey}
graph-snapshot	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph-snapshot/${ResourceId}`	aws:ResourceTag/${TagKey}
import-task	`arn:${Partition}:neptune-graph:${Region}:${Account}:import-task/${ResourceId}`	
export-task	`arn:${Partition}:neptune-graph:${Region}:${Account}:export-task/${ResourceId}`	

Clés de condition pour Amazon Neptune Analytics

Amazon Neptune Analytics définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString
neptune-graph:PublicConnectivity	Filtre l'accès en fonction de la valeur du paramètre de connectivité public fourni dans la demande ou de sa valeur par défaut, si elle n'est pas spécifiée. Tous les accès aux graphes sont authentifiés par IAM	Booléen

Actions, ressources et clés de condition pour AWS Network Firewall

AWS Network Firewall (préfixe de service :`network-firewall`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Network Firewall
- Types de ressources définis par AWS Network Firewall
- Clés de condition pour AWS Network Firewall

Actions définies par AWS Network Firewall

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptNetworkFirewallTransitGatewayAttachment	Autorise l'acceptation des pièces jointes Network Firewall en attente sur une passerelle de transit	Écrire	Firewall*		
AssociateAvailabilityZones	Accorde l'autorisation d'associer des zones de disponibilité à un pare-feu	Écrire	Firewall*		
AssociateFirewallPolicy	Accorde l'autorisation de créer une association entre une politique de pare-feu et un pare-feu	Écriture	Firewall*		
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateSubnets	Accorde l'autorisation d'associer des sous-réseaux de VPC à un pare-feu	Écrire	Firewall*		
AttachRuleGroupsToProxyConfiguration	Accorde l'autorisation d'associer des groupes de règles de proxy à une configuration de proxy	Écrire	ProxyConfiguration*		
			ProxyRuleGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFirewall	Autorise la création d'un pare-feu AWS Network Firewall	Écrire	Firewall*		iam:CreateServiceLinkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallPolicy	Autorise la création d'une politique de pare-feu AWS Network Firewall	Écrire	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateProxy	Autorise la création d'un proxy AWS Network Firewall	Écrire	Proxy*		ec2:AttachApplianceToNatGateway
			ProxyConfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProxyConfiguration	Accorde l'autorisation de créer une configuration de proxy AWS Network Firewall	Écrire	ProxyConfiguration*		
			ProxyRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProxyRuleGroup	Autorise la création d'un groupe de règles de proxy AWS Network Firewall	Écrire	ProxyRuleGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProxyRules	Accorde l'autorisation d'ajouter des règles de proxy à un groupe de règles de proxy	Écrire	ProxyRuleGroup*		
CreateRuleGroup	Autorise la création d'un groupe de règles AWS Network Firewall	Écrire	StatefulRuleGroup		
			StatelessRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTLSInspectionConfiguration	Accorde l'autorisation de créer une configuration d'inspection TLS du AWS Network Firewall	Écrire	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcEndpointAssociation	Accorde l'autorisation de créer une association de points de terminaison vpc AWS Network Firewall	Écrire	Firewall*		iam:CreateServiceLinkedRole
			VpcEndpointAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewall	Accorde l'autorisation de supprimer un pare-feu	Écriture	Firewall*		
DeleteFirewallPolicy	Accorde l'autorisation de supprimer une politique de pare-feu	Écrire	FirewallPolicy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteNetworkFirewallTransitGatewayAttachment	Autorise la suppression des pièces jointes du Network Firewall sur une passerelle de transit	Écrire	Firewall*		
DeleteProxy	Accorde l'autorisation de supprimer un proxy	Écrire	Proxy*		ec2:DetachApplianceFromNatGateway
DeleteProxyConfiguration	Accorde l'autorisation de supprimer une configuration de proxy	Écrire	ProxyConfiguration*		
DeleteProxyRuleGroup	Accorde l'autorisation de supprimer un groupe de règles de proxy	Écrire	ProxyRuleGroup*		
DeleteProxyRules	Accorde l'autorisation de supprimer des règles de proxy d'un groupe de règles de proxy	Écrire	ProxyRuleGroup*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressources pour une stratégie de pare-feu, un groupe de règles ou un pare-feu	Écrire	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			StatelessRuleGroup		
DeleteRuleGroup	Accorde l'autorisation de supprimer un groupe de règles	Écrire	StatefulRuleGroup*		
			StatelessRuleGroup*		
DeleteTLSInspectionConfiguration	Accorde l'autorisation de supprimer une configuration d'inspection TLS	Écrire	TLSInspectionConfiguration*		
DeleteVpcEndpointAssociation	Accorde l'autorisation de supprimer une association de point de terminaison VPC	Écrire	VpcEndpointAssociation*		
DescribeFirewall	Accorde l'autorisation de récupérer les objets de données qui définissent un pare-feu	Lecture	Firewall*		
DescribeFirewallMetadata	Accorde l'autorisation de récupérer les informations de haut niveau sur un pare-feu	Lecture	Firewall*		
DescribeFirewallPolicy	Accorde l'autorisation de récupérer les objets de données qui définissent une politique de pare-feu	Lecture	FirewallPolicy*		
			StatefulRuleGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			StatelessRuleGroup		
			TLSInspectionConfiguration		
DescribeFlowOperation	Accorde l'autorisation de décrire une opération de flux effectuée sur un pare-feu	Lecture	Firewall*		
DescribeLoggingConfiguration	Accorde l'autorisation de décrire la configuration de journalisation d'un pare-feu	Lecture	Firewall*		logs:GetLogDelivery logs:ListLogDeliveries
DescribeProxy	Accorde l'autorisation de récupérer les objets de données qui définissent un proxy	Lecture	Proxy*		
DescribeProxyConfiguration	Accorde l'autorisation de récupérer les objets de données qui définissent une configuration de proxy	Lecture	ProxyConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeProxyRule	Accorde l'autorisation de récupérer les objets de données qui définissent une règle de proxy	Lecture	ProxyRuleGroup*		
DescribeProxyRuleGroup	Accorde l'autorisation de récupérer les objets de données qui définissent un groupe de règles de proxy	Lecture	ProxyRuleGroup*		
DescribeResourcePolicy	Accorde l'autorisation de décrire une politique de ressources pour une stratégie de pare-feu, un groupe de règles ou un pare-feu	Lecture	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroup	Accorde l'autorisation de récupérer les objets de données qui définissent un groupe de règles	Lecture	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroupMetadata	Accorde l'autorisation de récupérer les informations de haut niveau à propos d'un groupe de règles	Lecture	StatefulRuleGroup		
			StatelessRuleGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRuleGroupSummary	Accorde l'autorisation de récupérer les informations récapitulatives concernant un groupe de règles	Lecture	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeTLSInspectionConfiguration	Accorde l'autorisation de récupérer les objets de données qui définissent une configuration d'inspection TLS	Lecture	TLSInspectionConfiguration*		
DescribeVpcEndpointAssociation	Accorde l'autorisation de récupérer les objets de données qui définissent une association de point de terminaison VPC	Lecture	VpcEndpointAssociation*		
DetachRuleGroupsFromProxyConfiguration	Accorde l'autorisation de détacher des groupes de règles de proxy d'une configuration de proxy	Écrire	ProxyConfiguration*		
			ProxyRuleGroup*		
DisassociateAvailabilityZones	Accorde l'autorisation de dissocier les zones de disponibilité d'un pare-feu	Écrire	Firewall*		
DisassociateSubnets	Accorde l'autorisation de dissocier les sous-réseaux VPC d'un pare-feu	Écrire	Firewall*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAnalysisReportResults	Accorde l'autorisation de récupérer les résultats des rapports d'analyse d'un pare-feu	Lecture	Firewall*		
ListAnalysisReports	Autorise à répertorier les rapports d'analyse du pare-feu	List	Firewall*		
ListFirewallPolicies	Accorde l'autorisation de récupérer les métadonnées pour les politiques de pare-feu	Liste	FirewallPolicy*		
ListFirewalls	Accorde l'autorisation de récupérer les métadonnées pour des pare-feu	List	Firewall*		
ListFlowOperationResults	Accorde l'autorisation de répertorier les résultats d'une opération de flux effectuée sur un pare-feu	Lecture	Firewall*		
ListFlowOperations	Accorde l'autorisation de répertorier les opérations de flux effectuées sur un pare-feu	List	Firewall*		
ListProxies	Accorde l'autorisation de récupérer les métadonnées pour les proxys	List	Proxy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProxyConfigurations	Accorde l'autorisation de récupérer les métadonnées pour les configurations de proxy	List	ProxyConfiguration*		
ListProxyRuleGroups	Accorde l'autorisation de récupérer les métadonnées pour les groupes de règles de proxy	List	ProxyRuleGroup*		
ListRuleGroups	Accorde l'autorisation de récupérer les métadonnées des groupes de règles	List			
ListTLSInspectionConfigurations	Accorde l'autorisation de récupérer les métadonnées des configurations d'inspection TLS	List	TLSInspectionConfiguration*		
ListTagsForResource	Accorde l'autorisation de récupérer les balises d'une ressource	List	Firewall*		
			FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			VpcEndpointAssociation		
ListVpcEndpointAssociations	Accorde l'autorisation de récupérer les métadonnées pour les associations de points de terminaison VPC	List	VpcEndpointAssociation*		
PutResourcePolicy	Accorde l'autorisation de définir une politique de ressources pour une stratégie de pare-feu, un groupe de règles ou un pare-feu	Écrire	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
RejectNetworkFirewallTransitGatewayAttachment	Autorise le rejet des pièces jointes Network Firewall en attente sur une passerelle de transit	Écrire	Firewall*		
StartAnalysisReport	Autorise le lancement d'un rapport d'analyse sur un pare-feu	Écrire	Firewall*		
StartFlowCapture	Autorise le lancement d'une opération de capture sur un pare-feu	Écrire	Firewall*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartFlowFlush	Autorise le lancement d'une opération de vidage sur un pare-feu	Écrire	Firewall*		
TagResource	Accorde l'autorisation d'attacher des balises à une ressource	Balisage	Firewall		
			FirewallPolicy		
			Proxy		
			ProxyConfiguration		
			ProxyRuleGroup		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	Firewall		
			FirewallPolicy		
			Proxy		
			ProxyConfiguration		
			ProxyRuleGroup		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateAvailabilityZoneChangeProtection	Accorde l'autorisation d'ajouter ou de supprimer une protection contre les modifications de zone de disponibilité pour un pare-feu	Écrire	Firewall*		
UpdateFirewallAnalysisSettings	Accorde l'autorisation de modifier les paramètres d'analyse du pare-feu d'un pare-feu	Écrire	Firewall*		
UpdateFirewallDeleteProtection	Accorde l'autorisation d'ajouter ou de supprimer une protection d'un pare-feu	Écriture	Firewall*		
UpdateFirewallDescription	Accorde l'autorisation de modifier la description d'un pare-feu	Écrire	Firewall*		
UpdateFirewallEncryptionConfiguration	Accorde l'autorisation de modifier la configuration de chiffrement d'un pare-feu	Écrire	Firewall*		
UpdateFirewallPolicy	Accorde l'autorisation de modifier une politique de pare-feu	Écriture	FirewallPolicy*		
			StatefulRuleGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Stateless RuleGroup		
			TLSInspectionConfiguration		
UpdateFirewallPolicyChangeProtection	Accorde l'autorisation d'ajouter ou de supprimer une protection contre les modifications d'une politique de pare-feu	Écriture	Firewall*		
UpdateLoggingConfiguration	Accorde l'autorisation de modifier la configuration de journalisation d'un pare-feu	Écrire	Firewall*		
UpdateProxy	Accorde l'autorisation de modifier un proxy	Écrire	Proxy*		
UpdateProxyConfiguration	Accorde l'autorisation de modifier la configuration d'un proxy	Écrire	ProxyConfiguration*		
UpdateProxyRule	Autorise la mise à jour d'une règle de proxy existante sur un groupe de règles de proxy	Écrire	ProxyRuleGroup*		
UpdateProxyRuleGroupPriorities	Accorde l'autorisation de modifier les priorités des groupes de règles dans une configuration de proxy	Écrire	ProxyConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateProxyRulePriorities	Accorde l'autorisation de mettre à jour les priorités des règles de proxy au sein d'un groupe de règles de proxy	Écrire	ProxyRuleGroup*		
UpdateRuleGroup	Accorde l'autorisation de modifier un groupe de règles	Écriture	StatefulRuleGroup		
			StatelessRuleGroup		
UpdateSubnetChangeProtection	Accorde l'autorisation d'ajouter ou de supprimer une protection contre les modifications de sous-réseau d'un pare-feu	Écrire	Firewall*		
UpdateTLSInspectionConfiguration	Accorde l'autorisation de modifier une configuration d'inspection TLS	Écrire	TLSInspectionConfiguration*		

Types de ressources définis par AWS Network Firewall

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Firewall	arn:${Partition}:network-firewall:${Region}:${Account}:firewall/${Name}	aws:ResourceTag/${TagKey}
FirewallPolicy	arn:${Partition}:network-firewall:${Region}:${Account}:firewall-policy/${Name}	aws:ResourceTag/${TagKey}
StatefulRuleGroup	arn:${Partition}:network-firewall:${Region}:${Account}:stateful-rulegroup/${Name}	aws:ResourceTag/${TagKey}
StatelessRuleGroup	arn:${Partition}:network-firewall:${Region}:${Account}:stateless-rulegroup/${Name}	aws:ResourceTag/${TagKey}
TLSInspectionConfiguration	arn:${Partition}:network-firewall:${Region}:${Account}:tls-configuration/${Name}	aws:ResourceTag/${TagKey}
VpcEndpointAssociation	arn:${Partition}:network-firewall:${Region}:${Account}:vpc-endpoint-association/${Name}	aws:ResourceTag/${TagKey}
ProxyRuleGroup	arn:${Partition}:network-firewall:${Region}:${Account}:proxy-rule-group/${Name}	aws:ResourceTag/${TagKey}
ProxyConfiguration	arn:${Partition}:network-firewall:${Region}:${Account}:proxy-configuration/${Name}	aws:ResourceTag/${TagKey}
Proxy	arn:${Partition}:network-firewall:${Region}:${Account}:proxy/${Name}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Network Firewall

AWS Network Firewall définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des étiquettes.	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur de balise associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Network Flow Monitor

Network Flow Monitor (préfixe de service :`networkflowmonitor`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Network Flow Monitor

- Types de ressources définis par Network Flow Monitor
- Clés de condition pour Network Flow Monitor

Actions définies par Network Flow Monitor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMonitor	Accorde la permission de créer un moniteur	Écrire	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScope	Accorde l'autorisation de créer une portée	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	Accorde la permission de supprimer un moniteur	Écrire	monitor*		
DeleteScope	Accorde l'autorisation de supprimer une portée	Écrire	scope*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMonitor	Accorde l'autorisation d'obtenir des informations sur un moniteur	Lecture	monitor*		
GetQueryResultsMonitorTopContributors	Accorde l'autorisation d'obtenir les résultats d'une requête qui récupère les données des principaux contributeurs pour un moniteur	Lecture	monitor*		
GetQueryResultsWorkloadInsightsTopContributors	Accorde l'autorisation d'obtenir les résultats d'une requête qui récupère les principaux contributeurs pour obtenir des informations sur la charge de travail	Lecture	scope*		
GetQueryResultsWorkloadInsightsTopContributorsData	Accorde l'autorisation d'obtenir les résultats d'une requête qui récupère les principaux points de données des contributeurs pour obtenir des informations sur la charge de travail	Lecture	scope*		
GetQueryStatusMonitorTopContributors	Accorde l'autorisation d'obtenir le statut d'une requête qui récupère les données des principaux contributeurs pour un moniteur	Lecture	monitor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQueryStatusWorkloadInsightsTopContributors	Accorde l'autorisation d'obtenir le statut d'une requête qui récupère les principaux contributeurs pour obtenir des informations sur la charge de travail	Lecture	scope*		
GetQueryStatusWorkloadInsightsTopContributorsData	Accorde l'autorisation d'obtenir le statut d'une requête qui extrait les points de données des principaux contributeurs pour obtenir des informations sur la charge de travail	Lecture	scope*		
GetScope	Accorde l'autorisation d'obtenir des informations sur un scope	Lecture	scope*		
ListMonitors	Accorde l'autorisation de répertorier tous les moniteurs d'un compte et leurs statuts	List			
ListScopes	Accorde l'autorisation d'obtenir tous les champs d'application d'un compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	monitor scope		
Publish	Autorise la publication d'un rapport	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartQueryMonitorTopContributors	Autorise le lancement d'une requête pour récupérer les données des principaux contributeurs pour un moniteur	Écrire	monitor*		
StartQueryWorkloadInsightsTopContributors	Autorise le lancement d'une requête pour récupérer les données des principaux contributeurs afin d'obtenir des informations sur la charge de travail	Écrire	scope*		
StartQueryWorkloadInsightsTopContributorsData	Autorise le lancement d'une requête pour récupérer les points de données des principaux contributeurs afin d'obtenir des informations sur la charge de travail	Écrire	scope*		
StopQueryMonitorTopContributors	Autorise l'arrêt d'une requête visant à récupérer les données des principaux contributeurs pour un moniteur	Écrire	monitor*		
StopQueryWorkloadInsightsTopContributors	Autorise l'arrêt d'une requête visant à récupérer les principaux contributeurs pour obtenir des informations sur la charge de travail	Écrire	scope*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopQueryWorkloadInsightsTopContributorsData	Autorise l'arrêt d'une requête visant à récupérer les points de données des principaux contributeurs pour obtenir des informations sur la charge de travail	Écrire	scope*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	monitor		
			scope		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	monitor		
			scope		
				aws:TagKeys	
UpdateMonitor	Accorde l'autorisation de mettre à jour un moniteur	Écrire	monitor*		
UpdateScope	Accorde l'autorisation de mettre à jour une portée	Écrire	scope*		

Types de ressources définis par Network Flow Monitor

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
monitor	`arn:${Partition}:networkflowmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
scope	`arn:${Partition}:networkflowmonitor:${Region}:${Account}:scope/${ScopeId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Network Flow Monitor

Network Flow Monitor définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtrer l'accès en fonction des clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Network Manager

AWS Network Manager (préfixe de service :`networkmanager`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le gestionnaire AWS de réseau
- Types de ressources définis par AWS Network Manager
- Clés de condition pour AWS Network Manager

Actions définies par le gestionnaire AWS de réseau

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptAttachment	Accorde l'autorisation d'accepter la création d'un attachement entre une source et une destination dans un réseau principal	Écrire	attachment*		ec2:DescribeRegions
AssociateConnectPeer	Accorde l'autorisation d'associer un pair Connect	Écrire	device*		
			global-network*		
AssociateCustomerGateway	Accorde l'autorisation d'associer une passerelle client à un appareil	Écriture	device*		
			global-network*		
			link		
				networkmanager:cgwArn	
AssociateLink	Accorde l'autorisation d'associer un lien à un appareil	Écriture	device*		
			global-network*		
			link*		
AssociateTransitGatewayConnectPeer	Accorde l'autorisation d'associer un pair Transit Gateway Connect à un appareil	Écrire	device*		
			global-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			link		
				networkmanager:tgwConnectPeerArn	
CreateConnectAttachment	Accorde l'autorisation de créer un attachement Connect	Écrire	attachment*		ec2:DescribeRegions networkmanager:TagResource
			core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectPeer	Accorde l'autorisation de créer une connexion de pair Connect	Écrire	attachment*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Accorde l'autorisation de créer une connexion	Écrire	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreNetwork	Accorde l'autorisation de créer un réseau principal	Écrire	global-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCoreNetworkPrefixListAssociation	Accorde l'autorisation de créer une association de réseau central avec une liste de préfixes	Écrire	core-network*		
CreateDevice	Accorde l'autorisation de créer un nouvel appareil	Écrire	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGatewayAttachment	Accorde l'autorisation de créer une pièce jointe à une passerelle Direct Connect	Écrire	core-network*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:directConnectGatewayArn networkmanager:edgeLocations	
CreateGlobalNetwork	Accorde l'autorisation de créer un nouveau réseau mondial	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole networkmanager:TagResource
CreateLink	Accorde l'autorisation de créer un nouveau lien	Écriture	global-network* site		networkmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSite	Accorde l'autorisation de créer un nouveau site	Écrire	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSiteToSiteVpnAttachment	Accorde l'autorisation de créer une pièce jointe site-to-site VPN	Écrire	core-network*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpnConnectionArn	
CreateTransitGatewayPeering	Accorde l'autorisation de créer un appairage de passerelle de transit	Écrire	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTransitGatewayRouteTableAttachment	Accorde l'autorisation de créer une annexe TGW RTB	Écrire	peering*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwRtbArn	
CreateVpcAttachment	Accorde l'autorisation de créer une annexe VPC	Écrire	core-network*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpcArn networkmanager:subnetArns	
DeleteAttachment	Accorde l'autorisation de supprimer une annexe	Écrire	attachment*		ec2:DescribeRegions
DeleteConnectPeer	Accorde l'autorisation de supprimer un pair Connect	Écrire	connect-peer*		ec2:DescribeRegions
DeleteConnection	Accorde l'autorisation de supprimer une connexion.	Écrire	connection*		
			global-network*		
DeleteCoreNetwork	Accorde l'autorisation de supprimer un réseau principal	Écrire	core-network*		ec2:DescribeRegions

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCoreNetworkPolicyVersion	Accorde l'autorisation de supprimer la version de politique de réseau principal	Écrire	core-network*		
DeleteCoreNetworkPrefixListAssociation	Autorise la suppression d'une liste de préfixes (association du réseau central)	Écrire	core-network*		
DeleteDevice	Accorde l'autorisation de supprimer un appareil	Écriture	device*		
			global-network*		
DeleteGlobalNetwork	Accorde l'autorisation de supprimer un réseau mondial	Écriture	global-network*		
DeleteLink	Accorde l'autorisation de supprimer un lien	Écrire	global-network*		
			link*		
DeletePeering	Accorde l'autorisation de supprimer un appairage	Écrire	peering*		ec2:DescribeRegions
DeleteResourcePolicy	Accorde l'autorisation de supprimer une ressource	Gestion des autorisations	core-network*		
DeleteSite	Accorde l'autorisation de supprimer un site	Écriture	global-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			site*		
DeregisterTransitGateway	Accorde l'autorisation de désenregistrer une passerelle de transit d'un réseau mondial	Écriture	global-network*		
				networkmanager:tgwArn	
DescribeGlobalNetworks	Accorde l'autorisation de décrire les réseaux mondiaux	List	global-network		
DisassociateConnectPeer	Accorde l'autorisation de dissocier un pair Connect	Écrire	global-network*		
DisassociateCustomerGateway	Accorde l'autorisation de dissocier une passerelle client d'un appareil	Écriture	global-network*		
				networkmanager:cgwArn	
DisassociateLink	Accorde l'autorisation de dissocier un lien d'un appareil	Écriture	device*		
			global-network*		
			link*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateTransitGatewayConnectPeer	Accorde l'autorisation de dissocier un paur Transit Gateway Connect d'un appareil	Écrire	global-network*		
				networkmanager:tgwConnectPeerArn	
ExecuteCoreNetworkChangeSet	Accorde l'autorisation d'appliquer des modifications au réseau principal	Écrire	core-network*		ec2:DescribeRegions
GetConnectAttachment	Accorde l'autorisation de récupérer un attachement Connect	Lecture	attachment*		
GetConnectPeer	Accorde l'autorisation de récupérer un pair Connect	Lecture	connect-peer*		
GetConnectPeerAssociations	Accorde l'autorisation de décrire les associations de pairs Connect	Lecture	global-network*		
GetConnections	Accorde l'autorisation de décrire les connexions	List	global-network*		
			connection		
GetCoreNetwork	Accorde l'autorisation de récupérer un réseau principal	Lecture	core-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCoreNetworkChangeEvents	Accorde l'autorisation de récupérer une liste des événements de modifications de réseau principal	Lecture	core-network*		
GetCoreNetworkChangeSet	Accorde l'autorisation de récupérer une liste des jeux de modifications de réseau principal	Lecture	core-network*		
GetCoreNetworkPolicy	Accorde l'autorisation de récupérer la politique de réseau principal	Lecture	core-network*		
GetCustomerGatewayAssociations	Accorde l'autorisation de décrire les associations de passerelles client	Liste	global-network*		
GetDevices	Accorde l'autorisation de décrire les appareils	List	global-network*		
			device		
GetDirectConnectGatewayAttachment	Autorise la récupération d'une pièce jointe à une passerelle Direct Connect	Lecture	attachment*		
GetLinkAssociations	Accorde l'autorisation de décrire les associations de liens	Liste	global-network*		
			device		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			link		
GetLinks	Accorde l'autorisation de décrire les liens	List	global-network*		
			link		
GetNetworkResourceCounts	Accorde l'autorisation de renvoyer le nombre de ressources pour un réseau mondial regroupé par type	Lecture	global-network*		
GetNetworkResourceRelationships	Accorde l'autorisation de récupérer des ressources associées pour une ressource au sein du réseau mondial	Lecture	global-network*		
GetNetworkResources	Accorde l'autorisation de récupérer une ressource du réseau mondial	Lecture	global-network*		
GetNetworkRoutes	Accorde l'autorisation de récupérer les routages d'une table de routage dans le réseau mondial	Lecture	global-network*		
GetNetworkTelemetry	Accorde l'autorisation de récupérer des objets de télémétrie réseau pour le réseau mondial	Lecture	global-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourcePolicy	Accorde l'autorisation de récupérer une politique de ressource.	Lecture	core-network*		
GetRouteAnalysis	Accorde l'autorisation de récupérer la configuration et le résultat d'une analyse de routage	Lecture	global-network*		
GetSiteToSiteVpnAttachment	Accorde l'autorisation de récupérer une pièce jointe site-to-site VPN	Lecture	attachment*		
GetSites	Accorde l'autorisation de décrire les réseaux mondiaux	Liste	global-network*		
			site		
GetTransitGatewayConnectPeerAssociations	Accorde l'autorisation de décrire les associations de pairs Transit Gateway Connect	List	global-network*		
GetTransitGatewayPeering	Accorde l'autorisation de récupérer un appairage de passerelle de transit	Lecture	peering*		
GetTransitGatewayRegistrations	Accorde l'autorisation de décrire les enregistrements de passerelles de transit	List	global-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTransitGatewayRouteTableAttachment	Accorde l'autorisation de récupérer une annexe TGW RTB	Lecture	attachment*		
GetVpcAttachment	Accorde l'autorisation de récupérer une annexe VPC	Lecture	attachment*		
ListAttachmentRoutingPolicyAssociations	Accorde l'autorisation de répertorier toutes les politiques de routage associées aux pièces jointes du réseau central	List	core-network*		
ListAttachments	Accorde l'autorisation de décrire les annexes	List	attachment*		
ListConnectPeers	Accorde l'autorisation de décrire les pairs Connect	List	connect-peer*		
ListCoreNetworkPolicyVersions	Accorde l'autorisation de répertorier les versions de politique de réseau principal	List	core-network*		
ListCoreNetworkPrefixListAssociations	Accorde l'autorisation de répertorier les associations de listes de préfixes du réseau principal	List	core-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCoreNetworkRoutingInformation	Accorde l'autorisation de répertorier les informations de routage du réseau principal	List	core-network*		
ListCoreNetworks	Accorde l'autorisation de répertorier les réseaux principaux	List			
ListOrganizationServiceAccessStatus	Accorde l'autorisation de répertorier le statut d'accès au service de l'organisation	List			
ListPeerings	Accorde l'autorisation de décrire les appairages	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource Network Manager	Lecture	attachment		
			connect-peer		
			connection		
			core-network		
			device		
			global-network		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			link		
			peering		
			site		
				aws:ResourceTag/${TagKey}	
PutAttachmentRoutingPolicyLabel	Accorde l'autorisation de mettre une étiquette de politique de routage des pièces jointes	Écrire	attachment*		
			core-network*		
PutCoreNetworkPolicy	Accorde l'autorisation de créer une politique de réseau principal	Écrire	core-network*		ec2:DescribeRegions
PutResourcePolicy	Accorde l'autorisation de créer ou de mettre à jour une politique de ressource	Gestion des autorisations	core-network*		
RegisterTransitGateway	Accorde l'autorisation d'enregistrer une passerelle de transit sur un réseau mondial	Écrire	global-network*		
				networkmanager:tgwArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RejectAttachment	Accorde l'autorisation de rejeter la demande d'annexe	Écrire	attachment*		
RemoveAttachmentRoutingPolicyLabel	Accorde l'autorisation de supprimer une étiquette de politique de routage des pièces jointes	Écrire	attachment*		
			core-network*		
RestoreCoreNetworkPolicyVersion	Accorde l'autorisation de restaurer la politique de réseau principal vers une version précédente.	Écrire	core-network*		ec2:DescribeRegions
StartOrganizationServiceAccessUpdate	Accorde l'autorisation de démarrer la mise à jour de l'accès au service de l'organisation	Gestion des autorisations			
StartRouteAnalysis	Accorde l'autorisation de démarrer une analyse de routage et stocke la configuration de l'analyse.	Écrire	global-network*		
TagResource	Accorde l'autorisation de baliser une ressource Network Manager	Balisage	attachment		
			connect-peer		
			connection		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource Network Manager	Balisage	attachment		
			connect-peer		
			connection		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys	
UpdateConnection	Accorde l'autorisation de mettre à jour une connexion.	Écrire	connection*		
			global-network*		
UpdateCoreNetwork	Accorde l'autorisation de mettre à jour un réseau principal	Écrire	core-network*		
UpdateDevice	Accorde l'autorisation de mettre à jour un appareil	Écrire	device*		
			global-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDirectConnectGatewayAttachment	Autorise la mise à jour d'une pièce jointe à une passerelle Direct Connect	Écrire	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:edgeLocations	
UpdateGlobalNetwork	Accorde l'autorisation de mettre à jour un réseau mondial	Écriture	global-network*		
UpdateLink	Accorde l'autorisation de mettre à jour un lien	Écrire	global-network*		
			link*		
UpdateNetworkResourceMetadata	Accorde l'autorisation d'ajouter ou de mettre à jour des key/value paires de métadonnées sur une ressource réseau	Écrire	global-network*		
UpdateSite	Accorde l'autorisation de mettre à jour un site	Écrire	global-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			site*		
UpdateVpcAttachment	Accorde l'autorisation de mettre à jour une annexe VPC	Écrire	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:subnetArns	

Types de ressources définis par AWS Network Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
global-network	`arn:${Partition}:networkmanager::${Account}:global-network/${ResourceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
site	arn:${Partition}:networkmanager::${Account}:site/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
link	arn:${Partition}:networkmanager::${Account}:link/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:networkmanager::${Account}:device/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
connection	arn:${Partition}:networkmanager::${Account}:connection/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
core-network	arn:${Partition}:networkmanager::${Account}:core-network/${ResourceId}	aws:ResourceTag/${TagKey}
attachment	arn:${Partition}:networkmanager::${Account}:attachment/${ResourceId}	aws:ResourceTag/${TagKey}
connect-peer	arn:${Partition}:networkmanager::${Account}:connect-peer/${ResourceId}	aws:ResourceTag/${TagKey}
peering	arn:${Partition}:networkmanager::${Account}:peering/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Network Manager

AWS Network Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
networkmanager:cgwArn	Filtre l'accès par lequel les passerelles client peuvent être associées ou dissociées	ARN
networkmanager:directConnectGatewayArn	Filtre l'accès par lequel la passerelle Direct Connect peut être utilisée pour une create/update pièce jointe	ARN
networkmanager:edgeLocations	Filtre l'accès en fonction duquel des emplacements périphériques peuvent être ajoutés ou supprimés d'une pièce jointe à une passerelle Direct Connect	ArrayOfString
networkmanager:subnetArns	Filtre l'accès par lequel des sous-réseaux VPC peuvent être ajoutés ou supprimés d'une annexe VPC	ArrayOfARN
networkmanager:tgwArn	Filtre l'accès par lequel les passerelles de transit peuvent être enregistrées, désenregistrées ou appairées	ARN
networkmanager:tgwConnectPeerArn	Filtre l'accès par lequel les pairs de connexion de passerelle de transit peuvent être associés ou dissociés	ARN

Clés de condition	Description	Type
networkmanager:tgwRtbArn	Filtre l'accès par lequel la table de routage de la passerelle de transit peut être utilisée pour créer une annexe	ARN
networkmanager:vpcArn	Filtre l'accès par lequel le VPC peut être utilisé pour une pièce jointe create/update	ARN
networkmanager:vpnConnectionArn	Filtre l'accès par lequel le Site-to-Site VPN peut être utilisé pour une create/update pièce jointe	ARN

Actions, ressources et clés de condition pour AWS Network Manager Chat

AWS Network Manager Chat (préfixe de service :`networkmanager-chat`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Network Manager Chat
- Types de ressources définis par AWS Network Manager Chat
- Clés de condition pour AWS Network Manager Chat

Actions définies par AWS Network Manager Chat

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelMessageResponse [autorisation uniquement]	Octroie l'autorisation d'annuler une réponse à un message.	Écrire			
CreateConversation [autorisation uniquement]	Octroie l'autorisation de créer une conversation.	Écrire			
DeleteConversation [autorisation uniquement]	Octroie l'autorisation de supprimer une conversation.	Écrire			
ListConversationMessages [autorisation uniquement]	Octroie l'autorisation de répertorier les messages de conversation.	List			
ListConversations [autorisation uniquement]	Octroie l'autorisation de répertorier les conversations.	List			
NotifyConversationIsActive	Octroie l'autorisation de signaler l'activité dans une conversation.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
SendConversationMessage [autorisation uniquement]	Octroie l'autorisation d'envoyer un message de conversation.	Écrire			

Types de ressources définis par AWS Network Manager Chat

AWS Network Manager Chat ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Network Manager Chat, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Network Manager Chat

Network Manager Chat ne comporte aucune clé de contexte propre au service pouvant être utilisée dans l'élément `Condition` des instructions de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Nimble Studio

Amazon Nimble Studio (préfixe de service : `nimble`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Nimble Studio
- Types de ressources définies par Amazon Nimble Studio
- Clés de condition pour Amazon Nimble Studio

Actions définies par Amazon Nimble Studio

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptEulas	Accorde l'autorisation d'accepter EULAs	Écrire	eula*		
CreateLaunchProfile	Accorde l'autorisation de créer un profil de lancement.	Écriture	studio*		ec2:CreateNetworkInterface ec2:DescribeNatGateways ec2:DescribeNetworkAcls

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:RunInstances
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateStreamingImage	Accorde l'autorisation de créer une image en streaming.	Écriture	studio*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute ec2:RegisterImage
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateStreamingSession	Accorde l'autorisation de créer une séance de streaming.	Écrire	launch-profile*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission nimble:GetLaunchProfile nimble:GetLaunchProfileInitialization nimble:ListEulaAcceptances
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingSessionStream	Accorde l'autorisation de créer un StreamingSessionStream	Écrire	streaming-session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				nimble:requesterPrincipalId	
CreateStudio	Accorde l'autorisation de créer un studio.	Écriture	studio*		iam:PassRole sso:CreateManagedApplicationInstance
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateStudioComponent	Accorde l'autorisation de créer un composant de studio. Un composant studio est une ressource réseau à laquelle un profil de lancement fournira l'accès.	Écriture	studio*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLaunchProfile	Accorde l'autorisation de supprimer un profil de lancement.	Écriture	launch-profile*		
DeleteLaunchProfileMember	Accorde l'autorisation de supprimer un membre du profil de lancement.	Écriture	launch-profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteStreamingImage	Accorde l'autorisation de supprimer une image en streaming.	Écriture	streaming-image*		ec2:DeleteSnapshot ec2:DeregisterImage ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute
DeleteStreamingSession	Accorde l'autorisation de supprimer une séance de streaming.	Écriture	streaming-session*		ec2:DeleteNetworkInterface
				nimble:requesterPrincipalId	
DeleteStudio	Accorde l'autorisation de supprimer un studio.	Écriture	studio*		sso:DeleteManagedApplicationInstance
DeleteStudioComponent	Accorde l'autorisation de supprimer un composant de studio.	Écriture	studio-component*		ds:UnauthorizeApplication

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteStudioMember	Accorde l'autorisation de supprimer un membre de studio.	Écriture	studio*		
GetEula	Accorde l'autorisation d'obtenir un CLUF.	Lecture	eula*		
GetFeatureMap [autorisation uniquement]	Accorde l'autorisation au portail Nimble Studio d'afficher les fonctions appropriées pour ce compte.	Lecture			
GetLaunchProfile	Accorde l'autorisation d'obtenir un profil de lancement.	Lecture	launch-profile*		
GetLaunchProfileDetails	Accorde l'autorisation d'obtenir des informations relatives à un profil de lancement, notamment le résumé des composants de studio et des images en streaming utilisés par le profil de lancement.	Lecture	launch-profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLaunchProfileInitialization	Accorde l'autorisation d'obtenir l'initialisation d'un profil de lancement. Une initialisation de profil de lancement est une version déréférencée d'un profil de lancement, y compris les informations de connexion d'un composant Studio attaché.	Lecture	launch-profile*		ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
GetLaunchProfileMember	Accorde l'autorisation d'obtenir un membre du profil de lancement.	Lecture	launch-profile*		
GetStreamingImage	Accorde l'autorisation d'obtenir une image en streaming.	Lecture	streaming-image*		
GetStreamingSession	Accorde l'autorisation d'obtenir une séance en streaming.	Lecture	streaming-session*		
				nimble:requesterPrincipalId	
GetStreamingSessionBackup	Accorde l'autorisation d'obtenir une sauvegarde de séance de streaming	Lecture	streaming-session-backup*		
				nimble:requesterPrincipalId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetStreamingSessionStream	Accorde l'autorisation d'obtenir un flux de séance en streaming.	Lecture	streaming-session*		
				nimble:requesterPrincipalId	
GetStudio	Accorde l'autorisation d'obtenir un studio.	Lecture	studio*		
GetStudioComponent	Accorde l'autorisation d'obtenir un composant de studio.	Lecture	studio-component*		
GetStudioMember	Accorde l'autorisation d'obtenir un membre de studio.	Lecture	studio*		
ListEulaAcceptances	Accorde l'autorisation de répertorier des acceptations de CLUF.	Lecture	eula-acceptance*		
ListEulas	Accorde l'autorisation de mettre en vente EULAs	Lecture	eula*		
ListLaunchProfileMembers	Accorde l'autorisation de répertorier des membres du profil de lancement.	Lecture	launch-profile*		
ListLaunchProfiles	Accorde l'autorisation de répertorier des profils de lancement.	Lecture	studio*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				nimble:principalId nimble:requesterPrincipalId	
ListStreamingImages	Accorde l'autorisation de répertorier des images en streaming.	Lecture	studio*		
ListStreamingSessionBackups	Accorde l'autorisation de répertorier des sauvegardes de séance de streaming	Lecture	studio*		
				nimble:requesterPrincipalId	
ListStreamingSessions	Accorde l'autorisation de répertorier des séances en streaming.	Lecture	studio*		
				nimble:createdBy nimble:ownedBy nimble:requesterPrincipalId	
ListStudioComponents	Accorde l'autorisation de répertorier des composants de studio.	Lecture	studio*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStudioMembers	Accorde l'autorisation de répertorier des membres du studio.	Lecture	studio*		
ListStudios	Accorde l'autorisation de répertorier tous les studios.	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises d'une ressource Nimble Studio.	Lecture	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		
PutLaunchProfileMembers	Accorde l'autorisation de add/update lancer des membres du profil	Écrire	launch-profile*		sso-directory:DescribeUsers

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutStudioLogEvents [autorisation uniquement]	Accorde l'autorisation de faire rapport sur les métriques et les journaux pour le portail Nimble Studio afin de surveiller l'état des applications.	Écrire	studio*		
PutStudioMembers	Accorde l'autorisation aux membres du add/update studio	Écrire	studio*		sso-directory:DescribeUsers
StartStreamingSession	Accorde l'autorisation de démarrer une séance en streaming	Écrire	streaming-session*		nimble:GetLaunchProfile nimble:GetLaunchProfileMember
			streaming-session-backup		
				nimble:requesterPrincipalId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartStudioSSOConfigurationRepair	Autorise la réparation de la configuration du centre d'identité AWS IAM du studio	Écrire	studio*		sso:CreateManagedApplicationInstance sso:GetManagedApplicationInstance
StopStreamingSession	Accorde l'autorisation d'arrêter une séance en streaming	Écrire	streaming-session*		nimble:GetLaunchProfile
				nimble:requesterPrincipalId	
TagResource	Accorde l'autorisation d'ajouter ou de remplacer une ou plusieurs balises pour la ressource Nimble Studio spécifiée.	Balisage	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			studio-component		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de dissocier une ou plusieurs balises de la ressource Nimble Studio spécifiée.	Balisage	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateLaunchProfile	Accorde l'autorisation de mettre à jour un profil de lancement.	Écriture	launch-profile*		ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints
UpdateLaunchProfileMember	Accorde l'autorisation de mettre à jour un membre du profil de lancement.	Écriture	launch-profile*		
UpdateStreamingImage	Accorde l'autorisation de mettre à jour une image en streaming.	Écriture	streaming-image*		
UpdateStudio	Accorde l'autorisation de mettre à jour un studio.	Écriture	studio*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateStudioComponent	Accorde l'autorisation de mettre à jour un composant de studio.	Écriture	studio-component*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole

Types de ressources définies par Amazon Nimble Studio

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
studio	arn:${Partition}:nimble:${Region}:${Account}:studio/${StudioId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
streaming-image	arn:${Partition}:nimble:${Region}:${Account}:streaming-image/${StreamingImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
studio-component	arn:${Partition}:nimble:${Region}:${Account}:studio-component/${StudioComponentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
launch-profile	arn:${Partition}:nimble:${Region}:${Account}:launch-profile/${LaunchProfileId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Types de ressources	ARN	Clés de condition
		nimble:studioId
streaming-session	arn:${Partition}:nimble:${Region}:${Account}:streaming-session/${StreamingSessionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:createdBy nimble:ownedBy
streaming-session-backup	arn:${Partition}:nimble:${Region}:${Account}:streaming-session-backup/${StreamingSessionBackupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:ownedBy
eula	arn:${Partition}:nimble:${Region}:${Account}:eula/${EulaId}	
eula-acceptance	arn:${Partition}:nimble:${Region}:${Account}:eula-acceptance/${EulaAcceptanceId}	nimble:studioId

Clés de condition pour Amazon Nimble Studio

Amazon Nimble Studio définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
nimble:createdBy	Filtre l'accès en fonction du paramètre de demande createdBy ou de l'ID du créateur de la ressource.	String
nimble:ownedBy	Filtre l'accès en fonction du paramètre de demande ownedBy ou de l'ID du propriétaire de la ressource	String
nimble:principalId	Filtre l'accès en fonction du paramètre de demande principalID.	String
nimble:requesterPrincipalId	Filtre l'accès en fonction de l'ID de l'utilisateur connecté	String
nimble:studioId	Filtre l'accès en fonction d'un studio spécifique	ARN

Actions, ressources et clés de condition pour Amazon Nova Act

Amazon Nova Act (préfixe de service :`nova-act`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Nova Act
- Types de ressources définis par Amazon Nova Act
- Clés de condition pour Amazon Nova Act

Actions définies par Amazon Nova Act

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAct	Accorde l'autorisation de créer une nouvelle tâche d'IA (act) au sein d'une session qui peut interagir avec des outils et effectuer des actions spécifiques	Écrire	workflow-definition*		
			workflow-run*		
CreateSession	Accorde l'autorisation de créer un nouveau contexte de session dans un flux de travail exécuté pour gérer l'état de la conversation et les actes	Écrire	workflow-definition*		
			workflow-run*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkflowDefinition	Accorde l'autorisation de créer un nouveau modèle de définition de flux de travail qui peut être utilisé pour exécuter plusieurs exécutions de flux de travail	Écrire	workflow-definition*		
CreateWorkflowRun	Accorde l'autorisation de créer une nouvelle instance d'exécution d'une définition de flux de travail avec des paramètres spécifiés	Écrire	workflow-definition*		
DeleteWorkflowDefinition	Accorde l'autorisation de supprimer une définition de flux de travail et toutes les ressources associées	Écrire	workflow-definition*		
DeleteWorkflowRun	Accorde l'autorisation de terminer et de nettoyer une exécution de flux de travail, en arrêtant tous les actes et sessions associés	Écrire	workflow-definition* workflow-run*		
GetWorkflowDefinition	Accorde l'autorisation de récupérer les détails et la configuration d'une définition de flux de travail spécifique	Lecture	workflow-definition*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkflowRun	Accorde l'autorisation de récupérer l'état actuel, la configuration et les détails d'exécution d'un flux de travail exécuté	Lecture	workflow-definition*		
			workflow-run*		
InvokeActStep	Accorde l'autorisation d'exécuter l'étape suivante d'un acte, de traiter les résultats des appels d'outils et de renvoyer de nouveaux appels d'outils si nécessaire	Écrire	workflow-definition*		
			workflow-run*		
ListActs	Permet de répertorier tous les actes d'une session spécifique avec leur statut actuel et les détails de leur exécution	Lecture	workflow-definition*		
ListModels	Accorde l'autorisation de répertorier tous les modèles d'IA disponibles pouvant être utilisés pour l'exécution du flux de travail, y compris leur statut et leurs informations de compatibilité	Lecture			
ListSessions	Accorde l'autorisation de répertorier toutes les sessions au sein d'une exécution de flux de travail spécifique	Lecture	workflow-definition*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workflow-run*		
ListWorkflowDefinitions	Accorde l'autorisation de répertorier toutes les définitions de flux de travail de votre compte avec filtrage et pagination facultatifs	List			
ListWorkflowRuns	Accorde l'autorisation de répertorier toutes les exécutions de flux de travail pour une définition de flux de travail spécifique avec filtrage et pagination facultatifs	List	workflow-definition*		
UpdateAct	Accorde l'autorisation de mettre à jour les informations de configuration, d'état ou d'erreur d'un acte existant	Écrire	workflow-definition*		
			workflow-run*		
UpdateWorkflowRun	Accorde l'autorisation de mettre à jour la configuration ou l'état d'un flux de travail actif exécuté	Écrire	workflow-definition*		
			workflow-run*		

Types de ressources définis par Amazon Nova Act

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workflow-definition	`arn:${Partition}:nova-act:${Region}:${Account}:workflow-definition/${WorkflowDefinitionName}`	
workflow-run	`arn:${Partition}:nova-act:${Region}:${Account}:workflow-definition/${WorkflowDefinitionName}/workflow-run/${WorkflowRunId}`	

Clés de condition pour Amazon Nova Act

Nova Act ne possède aucune clé de contexte spécifique à un service qui puisse être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon One Enterprise

Amazon One Enterprise (préfixe de service : `one`) fournit les ressources, actions et clés de contexte de condition propres au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon One Enterprise
- Types de ressources définis par Amazon One Enterprise
- Clés de condition pour Amazon One Enterprise

Actions définies par Amazon One Enterprise

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDeviceActivationQrCode	Octroie l'autorisation de créer un code QR pour une instance d'appareil.	Écrire	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateDeviceConfigurationTemplate	Octroie l'autorisation de créer un modèle de configuration d'appareil.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstance	Octroie l'autorisation de créer une instance d'appareil.	Écrire		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateDeviceInstanceConfiguration	Octroie l'autorisation de créer une configuration d'instance d'appareil.	Écrire	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateSite	Octroie l'autorisation de créer un site.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssociatedDevice	Octroie l'autorisation de dissocier un appareil d'une instance d'appareil.	Écrire	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceConfigurationTemplate	Octroie l'autorisation de supprimer un modèle de configuration d'appareil.	Écrire	device-configuration-template*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDeviceInstance	Octroie l'autorisation de supprimer une instance d'appareil.	Écrire	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteSite	Octroie l'autorisation de supprimer un site.	Écrire	site*		
				aws:ResourceTag/${TagKey}	
DeleteUserV1	Octroie l'autorisation de supprimer un utilisateur.	Écrire	user*		
GetDeviceConfigurationTemplate	Octroie l'autorisation d'afficher un modèle de configuration d'appareil.	Lecture	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstance	Octroie l'autorisation d'afficher une instance d'appareil.	Lecture	device-instance*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDeviceInstanceConfiguration	Octroie l'autorisation d'afficher une configuration d'instance d'appareil.	Lecture	configuration*		
				aws:ResourceTag/${TagKey}	
GetSite	Octroie l'autorisation d'afficher un site.	Lecture	site*		
				aws:ResourceTag/${TagKey}	
GetSiteAddress	Octroie l'autorisation d'afficher l'adresse d'un site.	Lecture	site*		
				aws:ResourceTag/${TagKey}	
ListDeviceConfigurationTemplates	Octroie l'autorisation de récupérer une liste de modèles de configuration d'appareil.	List			
ListDeviceInstances	Octroie l'autorisation de récupérer une liste d'instances d'appareils.	List			
ListSites	Octroie l'autorisation d'afficher une liste de sites.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Octroie l'autorisation de répertorier les balises d'une ressource Amazon One Enterprise.	Lecture	device-configuration-template		
			device-instance		
			site		
				aws:ResourceTag/${TagKey}	
ListUsers	Octroie l'autorisation d'afficher une liste d'utilisateurs.	List			
ListUsersV1	Octroie l'autorisation d'afficher une liste d'utilisateurs.	List			
RebootDevice	Octroie l'autorisation de redémarrer l'appareil associé à une instance d'appareil.	Écrire	device-instance*		
				aws:ResourceTag/${TagKey}	
TagResource	Octroie l'autorisation d'ajouter des balises à une ressource Amazon One Enterprise.	Identification	device-configuration-template		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			device-instance		
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Octroie l'autorisation de supprimer des balises d'une ressource Amazon One Enterprise.	Identification	device-configuration-template		
			device-instance		
			site		
				aws:TagKeys	
UpdateDeviceConfigurationTemplate	Octroie l'autorisation de mettre à jour un modèle de configuration d'appareil.	Écrire	device-configuration-template*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDeviceInstance	Octroie l'autorisation de mettre à jour une instance d'appareil.	Écrire	device-instance*		
				aws:ResourceTag/${TagKey}	
UpdateSite	Octroie l'autorisation de mettre à jour un site.	Écrire	site*		
				aws:ResourceTag/${TagKey}	
UpdateSiteAddress	Octroie l'autorisation de mettre à jour l'adresse d'un site.	Écrire	site*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon One Enterprise

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
device-instance	arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}	aws:ResourceTag/${TagKey}
configuration	arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}/configuration/${Version}	
device-configuration-template	arn:${Partition}:one:${Region}:${Account}:device-configuration-template/${TemplateId}	aws:ResourceTag/${TagKey}
site	arn:${Partition}:one:${Region}:${Account}:site/${SiteId}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:one:${Region}:${Account}:user/${UserId}	

Clés de condition pour Amazon One Enterprise

Amazon One Enterprise définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification dans la requête	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon OpenSearch

Amazon OpenSearch (préfixe de service :`opensearch`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon OpenSearch
- Types de ressources définis par Amazon OpenSearch
- Clés de condition pour Amazon OpenSearch

Actions définies par Amazon OpenSearch

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ApplicationAccessAll [autorisation uniquement]	Accorde l'autorisation d'accéder à OpenSearch l'application	Gestion des autorisations	application*		
CancelAutoOptimizeJob	Autorise l'annulation du Job Auto Optimize soumis	Écrire			
CancelDirectQuery	Accorde l'autorisation d'annuler la requête soumise sur la OpenSearch DataSource ressource	Écrire	datasource*		
DeleteAutoOptimizeJob	Accorde l'autorisation de supprimer Auto Optimize Job	Écrire			
GetAutoOptimizeJob	Accorde l'autorisation d'obtenir les détails d'Auto Optimize Job	Lecture			
GetDirectQuery	Accorde l'autorisation d'obtenir le statut des requêtes effectuées sur la OpenSearch DataSource ressource	Lecture	datasource*		
GetDirectQueryResult	Accorde l'autorisation d'obtenir les résultats d'une requête exécutée sur la OpenSearch DataSource ressource	Lecture	datasource*		
ListAutoOptimizeJobs	Accorde l'autorisation de récupérer une liste de tâches d'optimisation automatique	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDirectQuery	Accorde l'autorisation de lancer une requête directe sur les OpenSearch DataSource arns fournis	Écrire	datasource*		
SubmitAutoOptimizeJob	Accorde l'autorisation de créer un nouveau Job Auto Optimize	Écrire			

Types de ressources définis par Amazon OpenSearch

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}`	
datasource	`arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}`	

Clés de condition pour Amazon OpenSearch

OpenSearch ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion (préfixe de service :`osis`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon OpenSearch Ingestion
- Types de ressources définis par Amazon OpenSearch Ingestion
- Clés de condition pour Amazon OpenSearch Ingestion

Actions définies par Amazon OpenSearch Ingestion

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePipeline	Accorde l'autorisation de créer un pipeline OpenSearch d'ingestion	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:CreateLogDelivery
CreatePipelineEndpoint	Accorde l'autorisation de créer un point de terminaison du pipeline d' OpenSearch ingestion	Écrire	pipeline*		iam:CreateServiceLinkedRole
				aws:TagKeys aws:RequestTag/${TagKey}	
DeletePipeline	Autorise la suppression d'un pipeline OpenSearch d'ingestion	Écrire	pipeline*		logs:DeleteLogDelivery

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					logs:GetLogDelivery logs:ListLogDeliveries
DeletePipelineEndpoint	Autorise la suppression d'un point de terminaison du pipeline d' OpenSearch ingestion dans le compte courant	Écrire	pipeline-endpoint*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource pour une ressource d' OpenSearch ingestion	Écrire	pipeline*		
GetPipeline	Accorde l'autorisation de récupérer les informations de configuration pour un pipeline d' OpenSearch ingestion	Lecture	pipeline*		
GetPipelineBlueprint	Accorde l'autorisation d'obtenir le contenu d'un plan de pipeline d' OpenSearch ingestion	Lecture	pipeline-blueprint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPipelineChangeProgress	Accorde l'autorisation d'obtenir des informations détaillées sur l'état d'un pipeline d' OpenSearch ingestion	Lecture	pipeline*		
GetResourcePolicy	Accorde l'autorisation d'obtenir une politique de ressources pour une ressource d' OpenSearch ingestion	Lecture	pipeline*		
Ingest	Autorise l'ingestion de données via un pipeline d' OpenSearch ingestion	Écrire	pipeline*		
ListPipelineBlueprints	Accorde l'autorisation de répertorier les noms des plans disponibles pour une configuration de pipeline d' OpenSearch ingestion	List			
ListPipelineEndpointConnections	Accorde l'autorisation de répertorier les connexions des points de terminaison du pipeline d' OpenSearch ingestion aux pipelines du compte courant	List			
ListPipelineEndpoints	Permet de répertorier les points de terminaison du pipeline d' OpenSearch ingestion dans le compte courant	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPipelines	Accorde l'autorisation de répertorier la configuration de base pour chaque pipeline d' OpenSearch ingestion du compte courant et de la région	List			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises de ressources associées à un pipeline d' OpenSearch ingestion	Lecture	pipeline*		
PutResourcePolicy	Accorde l'autorisation de définir une politique de ressources pour une ressource d' OpenSearch ingestion	Écrire	pipeline*		
RevokePipelineEndpointConnections	Accorde l'autorisation de révoquer une connexion de point de terminaison du pipeline d' OpenSearch ingestion à partir d'un pipeline du compte courant	Écrire	pipeline*		
StartPipeline	Accorde l'autorisation de démarrer un pipeline OpenSearch d'ingestion	Écrire	pipeline*		
StopPipeline	Autorise l'arrêt d'un pipeline OpenSearch d'ingestion	Écrire	pipeline*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'attacher des balises de ressources à un pipeline d' OpenSearch ingestion	Identification	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises de ressources d'un pipeline de service d' OpenSearch ingestion	Identification	pipeline*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePipeline	Accorde l'autorisation de modifier la configuration d'un pipeline d' OpenSearch ingestion	Écrire	pipeline*		iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
ValidatePipeline	Accorde l'autorisation de valider la configuration d'un pipeline d' OpenSearch ingestion	Lecture			

Types de ressources définis par Amazon OpenSearch Ingestion

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
pipeline	`arn:${Partition}:osis:${Region}:${Account}:pipeline/${PipelineName}`	aws:ResourceTag/${TagKey}
pipeline-endpoint	`arn:${Partition}:osis:${Region}:${Account}:endpoint/${EndpointId}`	aws:ResourceTag/${TagKey}
pipeline-blueprint	`arn:${Partition}:osis:${Region}:${Account}:blueprint/${BlueprintName}`	

Clés de condition pour Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon OpenSearch Serverless

Amazon OpenSearch Serverless (préfixe de service :`aoss`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon OpenSearch Serverless
- Types de ressources définis par Amazon OpenSearch Serverless
- Clés de condition pour Amazon OpenSearch Serverless

Actions définies par Amazon OpenSearch Serverless

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
APIAccessAll	Accorder l'autorisation à tous les Opensearch pris en charge APIs	Écrire	Collection*		
				aoss:collection	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aoss:CollectionId	
AddCollectionToCollectionGroup	Accorde l'autorisation d'ajouter une collection sans serveur à un groupe de collecte spécifié	Écrire	CollectionGroup*		
				aoss:collection-group	
BatchGetCollection	Accorde l'autorisation d'obtenir des attributs pour une ou plusieurs collections	Lecture		aoss:collection	
BatchGetCollectionGroup	Accorde l'autorisation d'obtenir des attributs pour un ou plusieurs groupes de collections	Lecture		aoss:collection-group	
BatchGetEffectiveLifecyclePolicy	Accorde l'autorisation d'obtenir des informations sur une politique de cycle de vie appliquée à une ou plusieurs ressources AOSS	Lecture			
BatchGetLifecyclePolicy	Accorde l'autorisation d'obtenir des informations sur une ou plusieurs politiques de cycle de vie	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetVpcEndpoint	Accorde l'autorisation d'obtenir des attributs pour un ou plusieurs points de terminaison d'un VPC	Lecture			
CreateAccessPolicy	Accorde l'autorisation de créer une stratégie d'accès aux données	Écrire		aoss:collection aoss:index	
CreateCollection	Accorde l'autorisation de créer une collection sans serveur	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollectionGroup	Accorde l'autorisation de créer un groupe de collecte sans serveur	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Accorde l'autorisation de créer un index OpenSearch	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLifecyclePolicy	Accorde l'autorisation de créer une politique de cycle de vie	Écrire		aoss:index	
CreateSecurityConfig	Accorde l'autorisation de créer une configuration de sécurité sans serveur	Écrire			
CreateSecurityPolicy	Accorde l'autorisation de créer une politique de réseau ou de chiffrement	Écrire		aoss:collection	
CreateVpcEndpoint	Accorde l'autorisation de créer un point de OpenSearch-Serverless-managed terminaison VPC d'interface	Écrire			
DashboardsAccessAll	Accorde l'autorisation d'utiliser les tableaux de bord Opensearch sans serveur	Écrire	Dashboards*		
				aoss:collection aoss:CollectionId	
DeleteAccessPolicy	Accorde l'autorisation de supprimer une stratégie d'accès aux données	Écrire		aoss:collection aoss:index	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCollection	Accorde l'autorisation de supprimer une collection sans serveur	Écrire	Collection*		
DeleteCollectionGroup	Accorde l'autorisation de supprimer un groupe de collecte sans serveur	Écrire	CollectionGroup*		
DeleteIndex	Autorise la suppression d'un index OpenSearch	Écrire			
DeleteLifecyclePolicy	Accorde l'autorisation de supprimer une politique de cycle de vie	Écrire		aoss:index	
DeleteSecurityConfig	Accorde l'autorisation de supprimer une configuration de sécurité.	Écrire			
DeleteSecurityPolicy	Accorde l'autorisation de supprimer une politique de sécurité	Écrire		aoss:collection	
DeleteVpcEndpoint	Accorde l'autorisation de supprimer un point de terminaison VPC d' OpenSearch interface géré sans serveur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccessPolicy	Accorde l'autorisation d'obtenir des informations sur une stratégie d'accès aux données	Lecture		aoss:collection aoss:index	
GetAccountSettings	Accorde l'autorisation d'obtenir les paramètres du compte, y compris les paramètres de capacité	Lecture			
GetIndex	Accorde l'autorisation d'obtenir un index OpenSearch	Lecture			
GetPoliciesStats	Accorde l'autorisation d'obtenir des statistiques sur les politiques de sécurité de votre compte	Lecture			
GetSecurityConfig	Accorde l'autorisation d'obtenir des informations sur une configuration de sécurité sans serveur	Lecture			
GetSecurityPolicy	Accorde l'autorisation d'obtenir des informations sur une politique de sécurité	Lecture		aoss:collection	
ListAccessPolicies	Accorde l'autorisation de répertorier les stratégies d'accès aux données	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCollectionGroups	Accorde l'autorisation de répertorier les groupes de collections	List			
ListCollections	Accorde l'autorisation de répertorier les collections	List			
ListLifecyclePolicies	Accorde l'autorisation de répertorier les politiques de cycle de vie	List			
ListSecurityConfigs	Accorde l'autorisation de répertorier les configurations de sécurité	List			
ListSecurityPolicies	Accorde l'autorisation de répertorier les politiques de sécurité	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour une collection	List			
ListVpcEndpoints	Accorde l'autorisation de répertorier les points de OpenSearch terminaison VPC gérés sans serveur	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser une collection sans serveur	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises d'une collection	Écrire		aws:TagKeys	
UpdateAccessPolicy	Accorde l'autorisation de mettre à jour une stratégie d'accès aux données	Écrire		aoss:collection aoss:index	
UpdateAccountSettings	Accorde l'autorisation de mettre à jour les paramètres du compte, y compris les paramètres de capacité	Écrire			
UpdateCollection	Accorde l'autorisation de mettre à jour une collection	Écrire	Collection*		
UpdateCollectionGroup	Accorde l'autorisation de mettre à jour un groupe de collection	Écrire	CollectionGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateIndex	Autorise la mise à jour d'un index OpenSearch	Écrire			
UpdateLifecyclePolicy	Accorde l'autorisation de mettre à jour une politique de cycle de vie	Écrire		aoss:index	
UpdateSecurityConfig	Accorde l'autorisation de mettre à jour une configuration de sécurité	Écrire			
UpdateSecurityPolicy	Accorde l'autorisation de mettre à jour une politique de sécurité	Écrire		aoss:collection	
UpdateVpcEndpoint	Accorde l'autorisation de mettre à jour un point de OpenSearch terminaison VPC géré sans serveur	Écrire			

Types de ressources définis par Amazon OpenSearch Serverless

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Collection	`arn:${Partition}:aoss:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
CollectionGroup	`arn:${Partition}:aoss:${Region}:${Account}:collection-group/${CollectionGroupId}`	aws:ResourceTag/${TagKey}
Dashboards	`arn:${Partition}:aoss:${Region}:${Account}:dashboards/default`	

Clés de condition pour Amazon OpenSearch Serverless

Amazon OpenSearch Serverless définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aoss:CollectionId	Filtre l'accès en fonction de l'identifiant de la collection	String
aoss:collection	Filtre l'accès en fonction du nom de la collection	String
aoss:collection-group	Filtre l'accès en fonction du nom du groupe de collection	String
aoss:index	Filtre l'accès en fonction de l'index	String
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon OpenSearch Service

Amazon OpenSearch Service (préfixe de service `:es`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon OpenSearch Service
- Types de ressources définis par Amazon OpenSearch Service
- Clés de condition pour Amazon OpenSearch Service

Actions définies par Amazon OpenSearch Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptInboundConnection	Accorde l'autorisation au propriétaire d'un domaine de destination d'accepter une demande de connexion de recherche entre clusters entrante	Écrire			
AcceptInboundCrossClusterSearchConnection	Accorde l'autorisation au propriétaire d'un domaine de destination d'accepter une demande de connexion de recherche entre clusters entrante. Cette autorisation est obsolète. Utiliser à la AcceptInboundConnection place	Écrire			
AddDataSource	Accorde l'autorisation d'ajouter la source de données pour le domaine OpenSearch de service	Écrire	domain*		
AddDirectQueryDataSource	Accorde l'autorisation d'ajouter la source de données pour les OpenSearch arns fournis	Écrire	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTags	Accorde l'autorisation d'associer des balises de ressources à un domaine OpenSearch de service, à une source de données ou à une application	Identification	application*		
			datasource*		
			domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
Associate Package	Accorde l'autorisation d'associer un package à un domaine OpenSearch de service	Écrire	domain*		
Associate Packages	Accorde l'autorisation d'associer plusieurs packages à un domaine OpenSearch de service	Écrire	domain*		
Authorize VpcEndpointAccess	Accorde l'autorisation de fournir l'accès à un domaine Amazon OpenSearch Service via l'utilisation d'un point de terminaison VPC d'interface	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelDomainConfigChange	Accorde l'autorisation d'annuler une modification sur un domaine OpenSearch de service	Écrire	domain*		
CancelElasticsearchServiceSoftwareUpdate	Accorde l'autorisation d'annuler la mise à jour logicielle d'un domaine. Cette autorisation est obsolète. Utiliser à la CancelServiceSoftwareUpdate place	Écrire	domain*		
CancelServiceSoftwareUpdate	Accorde l'autorisation d'annuler la mise à jour logicielle d'un domaine	Écrire	domain*		
CreateApplication	Accorde l'autorisation de créer une OpenSearch application	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Accorde l'autorisation de créer un domaine Amazon OpenSearch Service	Écrire	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateElasticsearchDomain	Accorde l'autorisation de créer un domaine OpenSearch de service. Cette autorisation est obsolète. Utiliser à la CreateDomain place	Écrire	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchServiceRole	Accorde l'autorisation de créer le rôle lié au service requis pour les domaines de OpenSearch service qui utilisent l'accès VPC. Cette autorisation est obsolète. OpenSearch Le service crée pour vous le rôle lié au service	Écrire			
CreateIndex	Accorde l'autorisation de créer un index pour le domaine OpenSearch de service	Écrire	domain*		
CreateOutboundConnection	Accorde l'autorisation de créer une connexion de recherche entre clusters d'un domaine source vers un domaine de destination	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOutboundCrossClusterSearchConnection	Accorde l'autorisation de créer une connexion de recherche entre clusters d'un domaine source vers un domaine de destination. Cette autorisation est obsolète. Utiliser à la CreateOutboundConnection place	Écrire	domain*		
CreatePackage	Accorde l'autorisation d'ajouter un package à utiliser avec les domaines OpenSearch de service	Écrire			
CreateServiceRole	Accorde l'autorisation de créer le rôle lié au service requis pour les domaines Amazon OpenSearch Service qui utilisent un accès VPC	Écrire			
CreateVpcEndpoint	Accorde l'autorisation de créer un point de terminaison OpenSearch VPC géré par Amazon Service	Écrire			
DeleteApplication	Accorde l'autorisation de supprimer une OpenSearch application	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDataSource	Accorde l'autorisation de supprimer la source de données pour le domaine OpenSearch de service	Écrire	domain*		
DeleteDirectQueryDataSource	Accorde l'autorisation de supprimer la source de données pour les OpenSearch arns fournis	Écrire	datasource*		
DeleteDomain	Autorise la suppression d'un domaine Amazon OpenSearch Service et de toutes ses données	Écrire	domain*		
DeleteElasticsearchDomain	Accorde l'autorisation de supprimer un domaine de OpenSearch service et toutes ses données. Cette autorisation est obsolète. Utiliser à la DeleteDomain place	Écrire	domain*		
DeleteElasticsearchServiceRole	Accorde l'autorisation de supprimer le rôle lié au service requis pour les domaines de OpenSearch service qui utilisent l'accès VPC. Cette autorisation est obsolète. Utilisez l'API IAM pour supprimer les rôles lié à un service	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteInboundConnection	Accorde l'autorisation au propriétaire du domaine de destination de supprimer une connexion de recherche entre clusters entrante existante	Écrire			
DeleteInboundCrossClusterSearchConnection	Accorde l'autorisation au propriétaire du domaine de destination de supprimer une connexion de recherche entre clusters entrante existante. Cette autorisation est obsolète. Utiliser à la DeleteInboundConnection place	Écrire			
DeleteIndex	Autorise la suppression de l'index pour le domaine OpenSearch de service	Écrire	domain*		
DeleteOutboundConnection	Accorde l'autorisation au propriétaire du domaine source de supprimer une connexion de recherche entre clusters sortante existante	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteOutboundCrossClusterSearchConnection	Accorde l'autorisation au propriétaire du domaine source de supprimer une connexion de recherche entre clusters sortante existante. Cette autorisation est obsolète. Utiliser à la DeleteOutboundConnection place	Écrire			
DeletePackage	Accorde l'autorisation de supprimer un package du OpenSearch service. Le package ne peut pas être associé à aucun domaine	Écrire			
DeleteVpcEndpoint	Accorde l'autorisation de supprimer un point de terminaison VPC d' OpenSearch interface géré par Amazon Service	Écrire			
DescribeDomain	Accorde l'autorisation de consulter une description de la configuration de domaine pour le domaine de OpenSearch service spécifié, y compris l'ID du domaine, le point de terminaison du service et l'ARN	Lecture	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDomainAutoTunes	Accorde l'autorisation de consulter la configuration Auto-Tune du domaine pour le domaine de OpenSearch service spécifié, y compris l'état Auto-Tune et les calendriers de maintenance	Lecture	domain*		
DescribeDomainChangeProgress	Autorise l'affichage détaillé de la progression d'un domaine de OpenSearch service	Lecture	domain*		
DescribeDomainConfig	Accorde l'autorisation de consulter une description des options de configuration et de l'état d'un domaine de OpenSearch service	Lecture	domain*		
DescribeDomainHealth	Octroie l'autorisation de consulter les informations relatives à l'état du domaine et des nœuds, à la zone de disponibilité de secours, au nombre de nœuds par zone de disponibilité et au nombre de partitions par nœud.	Lecture	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDomainNodes	Accorde l'autorisation d'afficher les informations sur les nœuds configurés pour le domaine et leurs configurations : ID du nœud, type de nœud, état du nœud, zone de disponibilité, type d'instance et stockage	Lecture	domain*		
DescribeDomains	Accorde l'autorisation de consulter une description de la configuration du domaine pour un maximum de cinq domaines OpenSearch de service spécifiés	List	domain*		
DescribeDryRunProgress	Accorde l'autorisation de décrire l'état d'un contrôle de validation préalable à la mise à jour sur un domaine OpenSearch de service	Lecture	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeElasticsearchDomain	Accorde l'autorisation de consulter une description de la configuration de domaine pour le domaine de OpenSearch service spécifié, y compris l'ID du domaine, le point de terminaison du service et l'ARN. Cette autorisation est obsolète. Utiliser à la DescribeDomain place	Lecture	domain*		
DescribeElasticsearchDomainConfig	Accorde l'autorisation de consulter une description de la configuration et de l'état d'un domaine de OpenSearch service. Cette autorisation est obsolète. Utiliser à la DescribeDomainConfig place	Lecture	domain*		
DescribeElasticsearchDomains	Accorde l'autorisation de consulter une description de la configuration du domaine pour un maximum de cinq OpenSearch domaines Amazon spécifiés. Cette autorisation est obsolète. Utiliser à la DescribeDomains place	List	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeElasticsearchInstanceTypeLimits	Accorde l'autorisation de consulter le nombre d'instances, le stockage et les limites du nœud principal pour une OpenSearch version et un type d'instance donnés. Cette autorisation est obsolète. Utiliser à la DescribeInstanceTypeLimits place	List			
DescribeInboundConnections	Accorde l'autorisation de répertorier toutes les connexions de recherche entre clusters entrantes pour un domaine de destination	List			
DescribeInboundCrossClusterSearchConnections	Accorde l'autorisation de répertorier toutes les connexions de recherche entre clusters entrantes pour un domaine de destination. Cette autorisation est obsolète. Utiliser à la DescribeInboundConnections place	List			
DescribeInsightDetails	Accorde l'autorisation d'afficher des informations détaillées sur les informations relatives à un domaine OpenSearch de service	Lecture	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeInstanceTypeLimits	Accorde l'autorisation d'afficher le nombre d'instances, le stockage et les limites de nœud principal pour une version et un type d'instance de moteur donnés	List			
DescribeOutboundConnections	Accorde l'autorisation de répertorier toutes les connexions de recherche entre clusters sortantes pour un domaine source	List			
DescribeOutboundCrossClusterSearchConnections	Accorde l'autorisation de répertorier toutes les connexions de recherche entre clusters sortantes pour un domaine source. Cette autorisation est obsolète. Utiliser à la DescribeOutboundConnections place	List			
DescribePackages	Accorde l'autorisation de décrire tous les packages disponibles pour les domaines OpenSearch de service	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReservedElasticsearchInstanceOfferings	Accorde l'autorisation de récupérer les offres d'instances réservées pour Amazon OpenSearch Service. Cette autorisation est obsolète. Utiliser à la DescribeReservedInstanceOfferings place	List			
DescribeReservedElasticsearchInstances	Accorde l'autorisation de récupérer les instances réservées au OpenSearch service qui ont déjà été achetées. Cette autorisation est obsolète. Utiliser à la DescribeReservedInstances place	List			
DescribeReservedInstanceOfferings	Accorde l'autorisation de récupérer les offres d'instances réservées pour le service OpenSearch	List			
DescribeReservedInstances	Accorde l'autorisation de récupérer les instances réservées au OpenSearch service qui ont déjà été achetées	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeVpcEndpoints	Accorde l'autorisation de décrire un ou plusieurs points de terminaison OpenSearch VPC gérés par Amazon Service	List			
DissociatePackage	Accorde l'autorisation de dissocier un package du domaine de OpenSearch service spécifié	Écrire	domain*		
DissociatePackages	Accorde l'autorisation de dissocier plusieurs packages du domaine de OpenSearch service spécifié	Écrire	domain*		
ESCrossClusterGet	Accorde l'autorisation d'envoyer des demandes entre clusters à un domaine de destination	Lecture	domain		
ESHttpDelete	Accorde l'autorisation d'envoyer des requêtes HTTP DELETE au OpenSearch APIs	Écrire	domain		
ESHttpGet	Accorde l'autorisation d'envoyer des requêtes HTTP GET au OpenSearch APIs	Lecture	domain		
ESHttpHead	Accorde l'autorisation d'envoyer des requêtes HTTP HEAD au OpenSearch APIs	Lecture	domain		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ESHttpPatch	Accorde l'autorisation d'envoyer des requêtes HTTP PATCH au OpenSearch APIs	Écrire	domain		
ESHttpPost	Accorde l'autorisation d'envoyer des requêtes HTTP POST au OpenSearch APIs	Écrire	domain		
ESHttpPut	Accorde l'autorisation d'envoyer des requêtes HTTP PUT au OpenSearch APIs	Écrire	domain		
GetApplication	Accorde l'autorisation d'obtenir des informations sur une OpenSearch application	Lecture	application*		
GetCompatibleElasticsearchVersions	Accorde l'autorisation de récupérer une liste des versions compatibles OpenSearch et d'Elasticsearch vers lesquelles un domaine de OpenSearch service peut être mis à niveau. Cette autorisation est obsolète. Utiliser à la GetCompatibleVersions place	List	domain*		
GetCompatibleVersions	Accorde l'autorisation de récupérer la liste des versions de moteur compatibles vers lesquelles un domaine de OpenSearch service peut être mis à niveau	List	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataSource	Accorde l'autorisation d'obtenir la source de données pour le domaine OpenSearch de service	Lecture	domain*		
GetDefaultApplicationSetting	Accorde l'autorisation d'obtenir le paramètre d'application par défaut pour le OpenSearch service	Lecture	application*		
GetDirectQueryDataSource	Accorde l'autorisation d'obtenir la source de données pour les OpenSearch arns fournis	Lecture	datasource*		
GetDomainMaintenanceStatus	Accorde l'autorisation de récupérer l'état de l'action de maintenance pour le nœud.	Lecture	domain*		
GetIndex	Accorde l'autorisation d'obtenir un index pour le domaine OpenSearch de service	Lecture	domain*		
GetPackageVersionHistory	Accorde l'autorisation de récupérer l'historique des versions d'un package	Lecture			
GetUpgradeHistory	Accorde l'autorisation de récupérer l'historique de mise à niveau d'un domaine de OpenSearch service donné	Lecture	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetUpgradeStatus	Accorde l'autorisation de récupérer l'état de mise à niveau d'un domaine de OpenSearch service donné	Lecture	domain*		
ListApplications	Accorde l'autorisation de répertorier OpenSearch les applications	List	application*		
ListDataSources	Accorde l'autorisation de récupérer une liste de sources de données pour le domaine OpenSearch de service	List	domain*		
ListDirectQueryDataSources	Accorde l'autorisation de récupérer une liste de sources de données pour les OpenSearch arns fournis	List	datasource*		
ListDomainMaintenances	Accorde l'autorisation de récupérer une liste d'actions de maintenance pour le domaine OpenSearch de service	List	domain*		
ListDomainNames	Accorde l'autorisation d'afficher les noms de tous les domaines de OpenSearch service que possède l'utilisateur actuel	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDomainsForPackage	Accorde l'autorisation de répertorier tous les domaines de OpenSearch service auxquels un package est associé	List			
ListElasticsearchInstanceTypeDetails	Accorde l'autorisation de répertorier tous les types d'instances et les fonctionnalités disponibles pour une OpenSearch version donnée. Cette autorisation est obsolète. Utiliser à la ListInstanceTypeDetails place	List			
ListElasticsearchInstanceTypes	Accorde l'autorisation de répertorier tous les types d'instances EC2 pris en charge pour une version donnée OpenSearch	List			
ListElasticsearchVersions	Accorde l'autorisation de répertorier toutes les OpenSearch versions prises en charge sur Amazon OpenSearch Service. Cette autorisation est obsolète. Utiliser à la ListVersions place	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListInsights	Autorise le compte à répertorier les informations relatives aux domaines de OpenSearch service	List	domain		
ListInstanceTypeDetails	Accorde l'autorisation de répertorier tous les types d'instances et les fonctionnalités disponibles pour une version donnée OpenSearch ou Elasticsearch	List			
ListPackagesForDomain	Accorde l'autorisation de répertorier tous les packages associés au domaine OpenSearch de service	List	domain*		
ListScheduledActions	Accorde l'autorisation de récupérer une liste des modifications de configuration planifiées pour un domaine OpenSearch de service	List	domain*		
ListTags	Accorde l'autorisation d'afficher toutes les balises de ressources pour un domaine OpenSearch de service, une source de données ou une application	Lecture	application*		
			datasource*		
			domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListVersions	Accorde l'autorisation de répertorier toutes les versions prises en charge OpenSearch et d'Elasticsearch dans Amazon Service OpenSearch	List			
ListVpcEndpointAccess	Accorde l'autorisation de récupérer des informations sur chaque AWS principal autorisé à accéder à un domaine Amazon OpenSearch Service donné via l'utilisation d'un point de terminaison VPC d'interface	List			
ListVpcEndpoints	Accorde l'autorisation de récupérer tous les points de terminaison OpenSearch VPC gérés par Amazon Service dans la région et dans la région en cours Compte AWS	List			
ListVpcEndpointsForDomain	Accorde l'autorisation de récupérer tous les points de terminaison OpenSearch VPC gérés par Amazon Service associés à un domaine particulier	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PurchaseReservedElasticsearchInstanceOffering	Accorde l'autorisation d'acheter des instances réservées au OpenSearch service. Cette autorisation est obsolète. Utiliser à la PurchaseReservedInstanceOffering place	Écrire			
PurchaseReservedInstanceOffering	Accorde l'autorisation d'acheter des instances OpenSearch réservées	Écrire			
PutDefaultApplicationSetting	Accorde l'autorisation de définir ou de supprimer le paramètre d'application par défaut pour le OpenSearch service	Écrire	application*		
RejectInboundConnection	Accorde l'autorisation au propriétaire du domaine de destination de rejeter une demande de connexion de recherche entre clusters entrante	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RejectInboundCrossClusterSearchConnection	Accorde l'autorisation au propriétaire du domaine de destination de rejeter une demande de connexion de recherche entre clusters entrante. Cette autorisation est obsolète. Utiliser à la RejectInboundConnection place	Écrire			
RemoveTags	Accorde l'autorisation de supprimer les balises de ressources d'un domaine de OpenSearch service, d'une source de données ou d'une application	Identification	application*		
			datasource*		
			domain*		
				aws:TagKeys	
RevokeVpcEndpointAccess	Accorde l'autorisation de révoquer l'accès à un domaine Amazon OpenSearch Service fourni via un point de terminaison VPC d'interface	Écrire			
RollbackElasticsearchServiceSoftwareUpdate	Autorise l'annulation d'une mise à jour logicielle de service d'un domaine Elasticsearch vers sa version précédente	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RollbackServiceSoftwareUpdate	Autorise l'annulation d'une mise à jour logicielle de service d'un domaine OpenSearch vers sa version précédente	Écrire	domain*		
StartDomainMaintenance	Accorde l'autorisation de lancer la maintenance sur le nœud.	Écrire	domain*		
StartElasticsearchServiceSoftwareUpdate	Accorde l'autorisation de démarrer la mise à jour logicielle d'un domaine. Cette autorisation est obsolète. Utiliser à la StartServiceSoftwareUpdate place	Écrire	domain*		
StartServiceSoftwareUpdate	Accorde l'autorisation de démarrer la mise à jour logicielle d'un domaine	Écrire	domain*		
UpdateApplication	Autorise la mise à jour d'une OpenSearch application	Écrire	application*		
UpdateDataSource	Autorise la mise à jour de la source de données pour le domaine OpenSearch de service	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDirectQueryDataSource	Accorde l'autorisation de mettre à jour la source de données pour les OpenSearch arns fournis	Écrire	datasource*		
UpdateDomainConfig	Accorde l'autorisation de modifier la configuration d'un domaine de OpenSearch service, telle que le type d'instance ou le nombre d'instances	Écrire	domain*		
UpdateElasticsearchDomainConfig	Accorde l'autorisation de modifier la configuration d'un domaine de OpenSearch service, telle que le type d'instance ou le nombre d'instances. Cette autorisation est obsolète. Utiliser à la UpdateDomainConfig place	Écrire	domain*		
UpdateIndex	Autorise la mise à jour de l'index pour le domaine OpenSearch de service	Écrire	domain*		
UpdatePackage	Autorise la mise à jour d'un package à utiliser avec les domaines OpenSearch de service	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePackageScope	Accorde l'autorisation de mettre à jour la portée d'un package	Écrire			
UpdateScheduledAction	Accorde l'autorisation de replanifier une modification de configuration OpenSearch de domaine de service planifiée pour une date ultérieure	Écrire	domain*		
UpdateVpcEndpoint	Accorde l'autorisation de modifier un point de terminaison VPC d' OpenSearch interface géré par Amazon Service	Écrire			
UpgradeDomain	Accorde l'autorisation de lancer la mise à niveau d'un domaine de OpenSearch service vers une version donnée	Écrire	domain*		
UpgradeElasticsearchDomain	Accorde l'autorisation de lancer la mise à niveau d'un domaine de OpenSearch service vers une version spécifiée. Cette autorisation est obsolète. Utiliser à la UpgradeDomain place	Écrire	domain*		

Types de ressources définis par Amazon OpenSearch Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:es:${Region}:${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}`	aws:ResourceTag/${TagKey}
es_role	`arn:${Partition}:iam::${Account}:role/aws-service-role/es.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService`	aws:ResourceTag/${TagKey}
opensearchservice_role	`arn:${Partition}:iam::${Account}:role/aws-service-role/opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService`	aws:ResourceTag/${TagKey}
datasource	`arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon OpenSearch Service

Amazon OpenSearch Service définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS OpsWorks

AWS OpsWorks (préfixe de service :`opsworks`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS OpsWorks
- Types de ressources définis par AWS OpsWorks
- Clés de condition pour AWS OpsWorks

Actions définies par AWS OpsWorks

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssignInstance	Accorde l'autorisation d'affecter une instance enregistrée à une couche	Écrire	stack		
AssignVolume	Accorde l'autorisation d'affecter l'un des volumes Amazon EBS enregistrés de la pile à une instance spécifiée	Écrire	stack		
AssociateElasticIp	Accorde l'autorisation d'associer l'une des adresses IP Elastic enregistrées de la pile à une instance spécifiée	Écrire	stack		
AttachElasticLoadBalancer	Accorde l'autorisation d'attacher un équilibreur de charge Elastic Load Balancing à une couche spécifiée	Écrire	stack		
CloneStack	Accorde l'autorisation de créer un clone d'une pile spécifiée	Écrire	stack		
CreateApp	Accorde l'autorisation de créer une app pour une pile spécifiée	Écrire	stack		
CreateDeployment	Accorde l'autorisation d'exécuter des commandes de pile ou de déploiement	Écrire	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateInstance	Accorde l'autorisation de créer une instance dans une pile spécifiée	Écrire	stack		
CreateLayer	Accorde l'autorisation de créer une couche	Écrire	stack		
CreateStack	Accorde l'autorisation de créer une pile	Écrire			
CreateUserProfile	Accorde l'autorisation de créer un profil utilisateur	Écrire			
DeleteApp	Accorde l'autorisation de supprimer une app spécifiée	Écrire	stack		
DeleteInstance	Accorde l'autorisation de supprimer une instance spécifiée, ce qui arrête l'instance Amazon EC2 associée	Écrire	stack		
DeleteLayer	Accorde l'autorisation de supprimer une couche spécifiée	Écrire	stack		
DeleteStack	Accorde l'autorisation de supprimer une pile spécifiée	Écrire	stack		
DeleteUserProfile	Accorde l'autorisation de supprimer un profil utilisateur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterEcsCluster	Accorde l'autorisation de supprimer un profil utilisateur	Écrire	stack		
DeregisterElasticIp	Accorde l'autorisation d'annuler l'enregistrement d'une adresse IP élastique spécifiée	Écrire	stack		
DeregisterInstance	Accorde l'autorisation d'annuler l'enregistrement d'une instance Amazon EC2 ou d'une instance sur site enregistrée	Écrire	stack		
DeregisterRdsDbInstance	Accorde l'autorisation d'annuler l'enregistrement d'une instance Amazon RDS	Écrire	stack		
DeregisterVolume	Accorde l'autorisation d'annuler l'enregistrement d'un volume Amazon EBS	Écrire	stack		
DescribeAgentVersions	Accorde l'autorisation de décrire les versions AWS OpsWorks d'agent disponibles	List	stack		
DescribeApps	Accorde l'autorisation de demander la description d'un jeu d'apps spécifié	List	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCommands	Accorde l'autorisation de décrire les résultats de commandes spécifiées	List	stack		
DescribeDeployments	Accorde l'autorisation de demander la description d'un jeu de déploiements spécifié	List	stack		
DescribeEcsClusters	Accorde l'autorisation de décrire les clusters Amazon ECS enregistrés auprès d'une pile	List	stack		
DescribeElasticIps	Accorde l'autorisation de décrire une ou plusieurs adresses IP élastiques	List	stack		
DescribeElasticLoadBalancers	Accorde l'autorisation de décrire les instances Elastic Load Balancing d'une pile	List	stack		
DescribeInstances	Accorde l'autorisation de demander la description d'un jeu d'instances spécifié	List	stack		
DescribeLayers	Accorde l'autorisation de demander une description d'une ou de plusieurs couches dans une pile spécifiée	List	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeLoadBasedAutoScaling	Accorde l'autorisation de décrire les configurations de scalabilité automatique basées sur la charge pour les couches spécifiées	List	stack		
DescribeMyUserProfile	Accorde l'autorisation de décrire les informations SSH d'un utilisateur	List			
DescribeOperatingSystems	Accorde l'autorisation de décrire les systèmes d'exploitation pris en charge par AWS OpsWorks Stacks	List			
DescribePermissions	Accorde l'autorisation de décrire les autorisations pour une pile spécifiée	List	stack		
DescribeRaidArrays	Accorde l'autorisation de décrire les baies RAID d'une instance	List	stack		
DescribeRdsDbInstances	Accorde l'autorisation de décrire les instances Amazon RDS	List	stack		
DescribeServiceErrors	Accorde l'autorisation de décrire les erreurs AWS OpsWorks de service	List	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeStackProvisioningParameters	Accorde l'autorisation de demander une description des paramètres d'allocation d'une pile	List	stack		
DescribeStackSummary	Accorde l'autorisation de décrire le nombre de couches et d'applications dans une pile spécifiée, ainsi que le nombre d'instances dans chaque état, comme running_setup ou online	List	stack		
DescribeStacks	Accorde l'autorisation de demander une description d'une ou de plusieurs piles	List	stack		
DescribeTimeBasedAutoScaling	Accorde l'autorisation de décrire les configurations de scalabilité automatique basées sur l'heure pour les instances spécifiées	List	stack		
DescribeUserProfiles	Accorde l'autorisation de décrire les utilisateurs spécifiés	List			
DescribeVolumes	Accorde l'autorisation de décrire les volumes Amazon EBS d'une instance	List	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DetachElasticLoadBalancer	Accorde l'autorisation de détacher une instance Elastic Load Balancing spécifiée de sa couche	Écrire	stack		
DisassociateElasticIp	Accorde l'autorisation de dissocier une adresse IP élastique d'une instance	Écrire	stack		
GetHostnameSuggestion	Accorde l'autorisation d'obtenir un nom d'hôte généré pour la couche spécifiée, en fonction du thème du nom d'hôte actuel	Lecture	stack		
GrantAccess	Accorde l'autorisation d'accorder l'accès RDP à une instance Windows pour une durée déterminée	Écrire	stack		
ListTags	Accorde l'autorisation de renvoyer la liste des identifications appliquées à la pile ou à la couche spécifiée	List	stack		
RebootInstance	Accorde l'autorisation de redémarrer une instance spécifiée	Écrire	stack		
RegisterEcsCluster	Accorde l'autorisation d'enregistrer un cluster Amazon ECS spécifié auprès d'une pile	Écrire	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterElasticIp	Accorde l'autorisation d'enregistrer une adresse IP élastique auprès d'une pile spécifiée	Écrire	stack		
RegisterInstance	Accorde l'autorisation d'enregistrer des instances avec une pile spécifiée qui ont été créées en dehors de AWS OpsWorks	Écrire	stack		
RegisterRdsDbInstance	Accorde l'autorisation d'enregistrer une instance Amazon RDS auprès d'une pile	Écrire	stack		
RegisterVolume	Accorde l'autorisation d'enregistrer un volume Amazon EBS auprès d'une pile spécifiée	Écrire	stack		
SetLoadBasedAutoScaling	Accorde l'autorisation de spécifier la configuration de scalabilité automatique basée sur la charge pour une couche spécifiée	Écrire	stack		
SetPermission	Accorde l'autorisation de spécifier les autorisations d'un utilisateur	Gestion des autorisations	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetTimeBasedAutoScaling	spécifier la configuration de scalabilité automatique basée sur l'heure pour une instance spécifiée	Écrire	stack		
StartInstance	Accorde l'autorisation de démarrer une instance spécifiée	Écrire	stack		
StartStack	Accorde l'autorisation de démarrer les instances d'une pile	Écrire	stack		
StopInstance	Accorde l'autorisation d'arrêter une instance spécifiée	Écrire	stack		
StopStack	Accorde l'autorisation d'arrêter une pile spécifiée	Écrire	stack		
TagResource	Accorde l'autorisation d'appliquer des identifications à une couche ou à une pile spécifiée	Identification	stack		
UnassignInstance	Accorde l'autorisation d'annuler l'affectation d'une instance enregistrée de toutes ses couches	Écrire	stack		
UnassignVolume	Accorde l'autorisation d'annuler l'affectation d'un volume Amazon EBS affecté	Écrire	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer des identifications d'une couche ou à une pile spécifiée	Identification	stack		
UpdateApp	Accorde l'autorisation de mettre à jour une app spécifiée	Écrire	stack		
UpdateElasticIp	Accorde l'autorisation de mettre à jour le nom d'une adresse IP élastique enregistrée	Écrire	stack		
UpdateInstance	Accorde l'autorisation de mettre à jour une instance spécifiée	Écrire	stack		
UpdateLayer	Accorde l'autorisation de mettre à jour une couche spécifiée	Écrire	stack		
UpdateMyUserProfile	Accorde l'autorisation de mettre à jour la clé publique SSH d'un utilisateur	Écrire			
UpdateRdsDbInstance	Accorde l'autorisation de mettre à jour une instance Amazon RDS	Écrire	stack		
UpdateStack	Accorde l'autorisation de mettre à jour une pile spécifiée	Écrire	stack		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateUserProfile	Accorde l'autorisation de mettre à jour un profile utilisateur spécifié	Gestion des autorisations			
UpdateVolume	Accorde l'autorisation de mettre à jour le nom ou le point de montage d'un volume Amazon EBS	Écrire	stack		

Types de ressources définis par AWS OpsWorks

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
stack	`arn:${Partition}:opsworks:${Region}:${Account}:stack/${StackId}/`	

Clés de condition pour AWS OpsWorks

OpsWorks ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour la gestion AWS OpsWorks de la configuration

AWS OpsWorks La gestion de la configuration (préfixe de service :`opsworks-cm`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS OpsWorks Configuration Management
- Types de ressources définis par AWS OpsWorks Configuration Management
- Clés de condition pour la gestion AWS OpsWorks de la configuration

Actions définies par AWS OpsWorks Configuration Management

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate Node	Accorde l'autorisation d'associer un nœud à un serveur de gestion de configuration.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBackup	Accorde l'autorisation de créer une sauvegarde pour le serveur spécifié.	Écriture			
CreateServer	Accorde l'autorisation de créer un serveur.	Écriture			
DeleteBackup	Accorde l'autorisation de supprimer la sauvegarde spécifiée et éventuellement son compartiment S3.	Écrire			
DeleteServer	Accorde l'autorisation de supprimer le serveur spécifié avec sa CloudFormation pile correspondante et éventuellement le compartiment S3	Écrire			
DescribeAccountAttributes	Accorde l'autorisation de décrire des Service Limits du compte de l'utilisateur.	Liste			
DescribeBackups	Accorde l'autorisation de décrire une sauvegarde individuelle, toutes les sauvegardes d'un serveur spécifié ou toutes les sauvegardes du compte de l'utilisateur.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEvents	Accorde l'autorisation de décrire tous les événements du serveur spécifié.	Liste			
DescribeNodeAssociationStatus	Accorde l'autorisation de décrire le statut d'association pour le jeton de nœud spécifié et le serveur spécifié.	Liste			
DescribeServers	Accorde l'autorisation de décrire le serveur spécifié ou tous les serveurs du compte de l'utilisateur.	Liste			
DisassociateNode	Accorde l'autorisation de dissocier un nœud spécifié d'un serveur.	Écriture			
ExportServerEngineAttribute	Accorde l'autorisation d'exporter un attribut de moteur à partir d'un serveur.	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises appliquées au serveur ou à la sauvegarde spécifiés.	Lecture			
RestoreServer	Accorde l'autorisation d'appliquer une sauvegarde au serveur spécifié. Remplaces éventuellement l'instance EC2 si elle est spécifiée.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMaintenance	Accorde l'autorisation de démarrer immédiatement la maintenance du serveur.	Écriture			
TagResource	Accorde l'autorisation d'appliquer des balises au serveur ou à la sauvegarde spécifiés.	Balisage			
UntagResource	Accorde l'autorisation de supprimer des balises du serveur ou de la sauvegarde spécifiés	Balisage			
UpdateServer	Accorde l'autorisation de mettre à jour des paramètres généraux du serveur.	Écriture			
UpdateServerEngineAttributes	Accorde l'autorisation de mettre à jour des paramètres de serveur spécifiques au type de gestion de configuration.	Écrire			

Types de ressources définis par AWS OpsWorks Configuration Management

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
server	`arn:${Partition}:opsworks-cm::${Account}:server/${ServerName}/${UniqueId}`	
backup	`arn:${Partition}:opsworks-cm::${Account}:backup/${ServerName}-{Date-and-Time-Stamp-of-Backup}`	

Clés de condition pour la gestion AWS OpsWorks de la configuration

OpsworksCM ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les AWS Organizations

AWS Organizations (préfixe de service :`organizations`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les AWS Organisations
- Types de ressources définis par les AWS Organizations
- Clés de condition pour les AWS Organisations

Actions définies par les AWS Organisations

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptHandshake	Accorde l'autorisation d'envoyer une réponse à l'auteur d'une liaison pour accepter l'action proposée par la demande de liaison (handshake)	Écrire	handshake*		iam:CreateServiceLinkedRole
AttachPolicy	Accorde l'autorisation d'attacher une politique à une racine, une unité organisationnelle ou un compte individuel	Écrire	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
CancelHandshake	Accorde l'autorisation d'annuler une demande de liaison (handshake)	Écrire	handshake*		
CloseAccount	Accorde l'autorisation de fermer une organisat	Écrire	account*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	ion Compte AWS qui fait désormais partie d'une organisation, soit créée au sein de l'organisation, soit invitée à rejoindre l'organisation				
CreateAccount	Accorde l'autorisation de créer un Compte AWS membre automatiquement membre de l'organisation avec les informations d'identification à l'origine de la demande	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateGovCloudAccount	Accorde l'autorisation de créer un compte AWS GovCloud (américain)	Écrire		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOrganization	Accorde l'autorisation de créer une organisation. Le compte avec les informations d'identification qui appelle l' CreateOrganization opération devient automatiquement le compte de gestion de la nouvelle organisation.	Écrire			iam:CreateServiceLinkedRole
CreateOrganizationalUnit	Accorde l'autorisation de créer une unité organisationnelle (OU) au sein d'une unité organisationnelle racine ou parent	Écrire	organizationalunit		
			root		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePolicy	Accorde l'autorisation de créer une politique que vous pouvez associer à une racine, à une unité organisationnelle (UO) ou à un individu Compte AWS	Écrire		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeclineHandshake	Accorde l'autorisation de refuser une demande de liaison. Cette action définit l'état de la liaison sur DECLINED (REFUSÉ) et désactive effectivement la requête	Écrire	handshake*		
DeleteOrganization	Accorde l'autorisation de supprimer l'organisation	Écrire			
DeleteOrganizationalUnit	Accorde l'autorisation de supprimer une unité organisationnelle d'une unité organisationnelle racine ou d'une autre unité organisationnelle	Écrire	organizationalunit*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePolicy	Accorde l'autorisation de supprimer une politique de votre organisation	Écrire	policy*		
				organizations:PolicyType	
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de votre organisation	Écrire			
DeregisterDelegatedAdministrator	Accorde l'autorisation de désenregistrer le membre spécifié Compte AWS en tant qu'administrateur délégué pour le AWS service spécifié par ServicePrincipal	Écrire	account*		
				organizations:ServicePrincipal	
DescribeAccount	Accorde l'autorisation de récupérer les détails liés à Organizations sur le compte spécifié	Lecture	account*		
DescribeCreateAccountStatus	Accorde l'autorisation de récupérer le statut actuel d'une requête asynchrone pour créer un compte	Lecture			
DescribeEffectivePolicy	Accorde l'autorisation de récupérer la politique effective d'un compte	Lecture	account*		
				organizations:PolicyType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeHandshake	Accorde l'autorisation de récupérer les détails relatifs à une liaison demandée précédemment	Lecture	handshake*		
DescribeOrganization	Accorde l'autorisation de récupérer des informations sur l'organisation à laquelle appartiennent les informations d'identification de l'appel	Lecture			
DescribeOrganizationalUnit	Accorde l'autorisation de récupérer les détails relatifs à une unité organisationnelle (OU)	Lecture	organizationalunit*		
DescribePolicy	Accorde l'autorisation de récupérer les détails d'une politique	Lecture	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	Accorde l'autorisation d'obtenir des informations sur une politique de ressources	Lecture			
DescribeResponsibilityTransfer	Accorde l'autorisation de récupérer les informations relatives à un transfert de responsabilité antérieur	Lecture	responsibilitytransfer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				organizations:TransferType organizations:TransferDirection	
DetachPolicy	Accorde l'autorisation de détacher une politique d'une racine cible, d'une unité organisationnelle ou d'un compte	Écrire	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
DisableAWSServiceAccess	Accorde l'autorisation de désactiver l'intégration d'un AWS service (le service spécifié par ServicePrincipal) avec AWS Organizations	Écrire		organizations:ServicePrincipal	
DisablePolicyType	Accorde l'autorisation de désactiver un type de politique d'organisation dans une racine	Écrire	root*		
				organizations:PolicyType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableAWSServiceAccess	Accorde l'autorisation d'activer l'intégration d'un AWS service (le service spécifié par ServicePrincipal) avec AWS Organizations	Écrire		organizations:ServicePrincipal	
EnableAllFeatures	Accorde l'autorisation de démarrer le processus d'activation de toutes les fonctions dans une organisation, afin de la mettre à niveau pour qu'elle ne prenne pas seulement en charge les fonctions de facturation consolidée	Écrire			
EnablePolicyType	Accorde l'autorisation d'activer un type de politique dans une racine	Écrire	root*		
				organizations:PolicyType	
InviteAccountToOrganization	Accorde l'autorisation d'envoyer une invitation à une autre Compte AWS personne, en lui demandant de rejoindre votre organisation en tant que compte membre	Écrire	account		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InviteOrganizationToTransferResponsibility	Accorde l'autorisation d'envoyer une invitation à une autre personne Compte AWS, lui demandant de transférer une responsabilité particulière à votre organisation	Écrire	account		
				organizations:TransferType organizations:TransferDirection	
LeaveOrganization	Accorde l'autorisation de supprimer un compte membre de son organisation parent	Écrire			
ListAWSServiceAccessForOrganization	Accorde l'autorisation de récupérer la liste des AWS services pour lesquels vous avez activé l'intégration dans votre organisation	List			
ListAccounts	Permet de répertorier tous les comptes de l'organisation	List			
ListAccountsForParent	Accorde l'autorisation de répertorier les comptes d'une organisation qui se trouvent dans une racine ou une unité organisationnelle (OU)	List	organizationalunit		
			root		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAccountsWithInvalidEffectivePolicy	Accorde l'autorisation de répertorier les comptes dont les politiques efficaces ne sont pas valides pour un type de stratégie spécifié	List		organizations:PolicyType	
ListChildren	Accorde l'autorisation de répertorier tous les comptes OUs ou contenus dans une unité d'organisation parent ou racine	List	organizationalunit root		
ListCreateAccountStatus	Accorde l'autorisation de répertorier les demandes de création de compte asynchrones qui font actuellement l'objet d'un suivi pour l'organisation	List			
ListDelegatedAdministrators	Accorde l'autorisation de répertorier les AWS comptes désignés comme administrateurs délégués dans cette organisation	List		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	Accorde l'autorisation de répertorier les AWS services pour lesquels le compte spécifié est un administrateur délégué dans cette organisation	List	account*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEffectivePolicyValidationErrors	Accorde l'autorisation de répertorier les erreurs de validation détectées dans la politique effective pour un compte et un type de politique spécifiques	List	account*		
				organizations:PolicyType	
ListHandshakesForAccount	Accorde l'autorisation de répertorier toutes les liaisons qui sont associées à un compte	List			
ListHandshakesForOrganization	Accorde l'autorisation de répertorier les liaisons qui sont associées à l'organisation	List			
ListInboundResponsibilityTransfers	Permet de répertorier toutes les responsabilités d'un type particulier transférées à votre organisation	List		organizations:TransferType organizations:TransferDirection	
ListOrganizationalUnitsForParent	Accorde l'autorisation de répertorier toutes les unités organisationnelles (OUs) d'une unité organisationnelle parent ou racine	List	organizationalunit		
			root		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOutboundResponsibilityTransfers	Permet de répertorier toutes les responsabilités d'un type particulier transférées à une autre organisation	List		organizations:TransferType organizations:TransferDirection	
ListParents	Accorde l'autorisation de répertorier la racine ou les unités organisationnelles (OUs) qui servent de parent immédiat à une unité d'organisation ou à un compte enfant	List	account		
			organizationalunit		
ListPolicies	Accorde l'autorisation de répertorier toutes les stratégies d'une organisation	List		organizations:PolicyType	
ListPoliciesForTarget	Accorde l'autorisation de répertorier toutes les stratégies qui sont attachées directement à une racine, une unité organisationnelle (OU) ou un compte	List	account		
			organizationalunit		
			root		
				organizations:PolicyType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRoots	Accorde l'autorisation de répertorier toutes les racines qui sont définies dans l'organisation	List			
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises pour la ressource spécifiée	List	account		
			organizationalunit		
			policy		
			resourcepolicy		
			responsibilitytransfer	organizations:TransferType	
				organizations:TransferDirection	
			root		
				organizations:PolicyType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTargetsForPolicy	Accorde l'autorisation de répertorier toutes OUs les racines et tous les comptes auxquels une politique est attachée	List	policy*		
				organizations:PolicyType	
MoveAccount	Accorde l'autorisation de déplacer un compte de sa racine ou unité organisationnelle actuelle vers une autre racine ou unité organisationnelle parent	Écrire	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	Accorde l'autorisation de créer ou de mettre à jour une politique de ressource	Écrire	resourcepolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDelegatedAdministrator	Accorde l'autorisation d'enregistrer le compte de membre spécifié pour administrer les fonctionnalités du AWS service Organizations spécifié par ServicePrincipal	Écrire	account*		
				organizations:ServicePrincipal	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveAccountFromOrganization	Accorde l'autorisation de supprimer le compte spécifié de l'organisation	Écrire	account*		
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs identifications à la ressource spécifiée	Identification	account		
			organizationalunit		
			policy	organizations:PolicyType	
			resourcepolicy		
			responsibilitytransfer	organizations:TransferType organizations:TransferDirection	
			root		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} organizations:PolicyType	
TerminateResponsibilityTransfer	Accorde l'autorisation de mettre fin au transfert d'une responsabilité vers ou depuis votre organisation	Écrire	responsibilitytransfer*		
				organizations:TransferType organizations:TransferDirection	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs identifications de la ressource spécifiée	Identification	account		
			organizationalunit		
			policy		
			resourcepolicy		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			responsibilitytransfer	organizations:TransferType organizations:TransferDirection	
			root		
				aws:TagKeys organizations:PolicyType	
UpdateOrganizationalUnit	Accorde l'autorisation de renommer une unité organisationnelle (OU)	Écrire	organizationalunit*		
UpdatePolicy	Accorde l'autorisation de mettre à jour une politique existante avec un nouveau nom, une nouvelle description ou un nouveau contenu	Écrire	policy*		
				organizations:PolicyType	
UpdateResponsibilityTransfer	Accorde l'autorisation de renommer un transfert de responsabilité vers ou depuis votre organisation	Écrire	responsibilitytransfer*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				organizations:TransferType organizations:TransferDirection	

Types de ressources définis par les AWS Organizations

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
account	`arn:${Partition}:organizations::${Account}:account/o-${OrganizationId}/${AccountId}`	aws:ResourceTag/${TagKey}
handshake	`arn:${Partition}:organizations::${Account}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}`	

Types de ressources	ARN	Clés de condition
organization	arn:${Partition}:organizations::${Account}:organization/o-${OrganizationId}	
organizationalunit	arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}	aws:ResourceTag/${TagKey}
resourcepolicy	arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}	aws:ResourceTag/${TagKey}
awspolicy	arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}	
root	arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}	aws:ResourceTag/${TagKey}
responsibilitytransfer	arn:${Partition}:organizations::${Account}:transfer/o-${OrganizationId}/${TransferType}/${TransferDirection}/rt-${ResponsibilityTransferId}	aws:ResourceTag/${TagKey}

Clés de condition pour les AWS Organisations

AWS Organizations définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
organizations:PolicyType	Filtre l'accès en fonction du type de tâche spécifié	String
organizations:ServicePrincipal	Filtre l'accès en fonction du service principal spécifié	String
organizations:TransferDirection	Filtre l'accès en fonction de la responsabilité spécifiée (transfert par la direction)	String
organizations:TransferType	Filtre l'accès en fonction des noms de type de transfert de responsabilité spécifiés	String

Actions, ressources et clés de condition pour les AWS Outposts

AWS Outposts (préfixe de service :`outposts`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Outposts
- Types de ressources définis par AWS Outposts
- Clés de condition pour AWS Outposts

Actions définies par AWS Outposts

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelCapacityTask	Accorde l'autorisation d'annuler une tâche de capacité	Écrire	outpost*		
CancelOrder	Accorde l'autorisation d'annuler une commande	Écrire			
CreateOrder	Accorde l'autorisation de créer une ordre.	Écrire	outpost*		
CreateOutpost	Accorde l'autorisation de créer un Outpost.	Écrire	site*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreatePrivateConnectivityConfig	Accorde l'autorisation de créer une configuration de connectivité privée.	Écrire	outpost*		
CreateSite	Accorde l'autorisation de créer un site	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteOutpost	Accorde l'autorisation de supprimer un Outpost.	Écrire	outpost*		
DeleteSite	Accorde l'autorisation de supprimer un site	Écrire	site*		
GetCapacityTask	Accorde l'autorisation d'obtenir des informations sur la tâche de capacité spécifiée	Lecture	outpost*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCatalogItem	Accorde l'autorisation d'obtenir un élément de catalogue	Lecture			
GetConnection	Accorde l'autorisation d'obtenir les informations sur la connection pour les servers Outpost	Lecture			
GetOrder	Accorde l'autorisation d'obtenir des informations sur une commande	Lecture			
GetOutpost	Accorde l'autorisation d'obtenir les informations sur l'Outpost spécifié	Lecture	outpost*		
GetOutpostBillingInformation	Accorde l'autorisation d'obtenir les informations de facturation d'Outpost pour l'Outpost spécifié	Lecture	outpost*		
GetOutpostInstanceTypes	Accorde l'autorisation d'obtenir les types d'instance de l'Outpost spécifié	Lecture	outpost*		
GetOutpostSupportedInstanceTypes	Accorde l'autorisation d'obtenir les types d'instances pris en charge pour l'avant-poste spécifié	Lecture	outpost*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPrivateConnectivityConfig	Accorde l'autorisation d'obtenir une configuration de connectivité privée.	Lecture	outpost*		
GetSite	Accorde l'autorisation d'obtenir un site	Lecture	site*		
GetSiteAddress	Accorde l'autorisation d'obtenir une adresse de site	Lecture	site*		
ListAssetInstances	Accorde l'autorisation de répertorier toutes les instances en cours d'exécution pour l'avant-poste spécifié	List	outpost*		
ListAssets	Accorde l'autorisation de répertorier les ressources pour votre Outpost	List	outpost*		
ListBlockingInstancesForCapacityTask	Accorde l'autorisation de répertorier toutes les instances en cours d'exécution qui bloquent l'exécution de la tâche de capacité pour l'avant-poste spécifié	List	outpost*		
ListCapacityTasks	Accorde l'autorisation de répertorier les tâches de capacité pour votre Compte AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCatalogItems	Accorde l'autorisation de répertorier tous les éléments de catalogue	List			
ListOrders	Accorde l'autorisation de répertorier les commandes pour votre Compte AWS	List			
ListOutposts	Accorde l'autorisation de répertorier les Outposts pour votre Compte AWS	List			
ListSites	Accorde l'autorisation de répertorier les sites pour votre Compte AWS	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture			
StartCapacityTask	Accorde l'autorisation de créer une tâche de capacité	Écrire	outpost*		
StartConnection	Accorde l'autorisation de démarrer une connection pour les servers Outpost	Écrire			
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	outpost		
			site		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	outpost		
			site		
				aws:TagKeys	
UpdateOutpost	Accorde l'autorisation de mettre à jour un Outpost	Écrire	outpost*		
UpdateSite	Accorde l'autorisation de mettre à jour un site	Écrire	site*		
UpdateSiteAddress	Accorde l'autorisation de mettre à jour l'adresse du site	Écrire	site*		
UpdateSiteRackPhysicalProperties	Accorde l'autorisation de mettre à jour les propriétés physiques d'un rack dans un site	Écrire	site*		

Types de ressources définis par AWS Outposts

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
outpost	`arn:${Partition}:outposts:${Region}:${Account}:outpost/${OutpostId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:outposts:${Region}:${Account}:site/${SiteId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Outposts

AWS Outposts définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Panorama

AWS Panorama (préfixe de service :`panorama`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Panorama
- Types de ressources définis par AWS Panorama
- Clés de condition pour AWS Panorama

Actions définies par AWS Panorama

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApplicationInstance	Autorise la création d'une instance d'application AWS Panorama	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateJobForDevices	Autorise la création d'une tâche pour un appareil AWS Panorama	Écrire			
CreateNodeFromTemplateJob	Autorise la création d'un nœud AWS Panorama	Écrire			
CreatePackage	Autorise la création d'un Package AWS Panorama	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePackageImportJob	Autorise la création d'un Package AWS Panorama	Écrire			
DeleteDevice	Autorise le désenregistrement d'un appareil Panorama AWS	Écrire	device*		
DeletePackage	Autorise la suppression d'un Package AWS Panorama	Écrire	package*		
DeregisterPackageVersion	Autorise le désenregistrement d'une version du package AWS Panorama	Écrire	package*		
DescribeApplicationInstance	Autorise l'affichage des informations relatives à une instance d'application AWS Panorama	Lecture	applicationInstance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeApplicationInstanceDetails	Autorise l'affichage des informations relatives à une instance d'application AWS Panorama	Lecture	applicationInstance*		
DescribeDevice	Autorise l'accès aux informations relatives à un appareil AWS Panorama	Lecture	device*		
DescribeDeviceJob	Permet de consulter les détails de la tâche pour un appareil AWS Panorama	Lecture			
DescribeNode	Autorise l'affichage des informations relatives à un nœud d'application AWS Panorama	Lecture			
DescribeNodeFromTemplateJob	Autorise l'accès aux informations relatives au nœud de l'application AWS Panorama	Lecture			
DescribePackage	Autorise l'accès aux détails d'un forfait AWS Panorama	Lecture	package*		
DescribePackageImportJob	Autorise l'accès aux détails d'un forfait AWS Panorama	Lecture			
DescribePackageVersion	Autorise l'accès aux détails d'une version du package AWS Panorama	Lecture	package*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSoftware [autorisation uniquement]	Autorise l'affichage des informations relatives à une version logicielle de l'appareil AWS Panorama	Lecture			
GetWebSocketURL [autorisation uniquement]	Accorde l'autorisation de générer un WebSocket point de terminaison pour communiquer avec AWS Panorama	Lecture			
ListApplicationInstanceDependencies	Accorde l'autorisation de récupérer une liste des dépendances des instances d'application dans AWS Panorama	List	applicationInstance*		
ListApplicationInstanceNodeInstances	Accorde l'autorisation de récupérer une liste d'instances de nœuds d'applications dans AWS Panorama	List	applicationInstance*		
ListApplicationInstances	Autorise la récupération d'une liste d'instances d'applications dans AWS Panorama	List	device		
ListDevices	Autorise la récupération d'une liste d'appareils dans AWS Panorama	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDevicesJobs	Permet de récupérer une liste de tâches pour un appareil AWS Panorama	List	device		
ListNodeFromTemplateJobs	Accorde l'autorisation de récupérer une liste de nœuds pour un appareil AWS Panorama	List			
ListNodes	Accorde l'autorisation de récupérer une liste de nœuds dans AWS Panorama	List			
ListPackageImportJobs	Permet de récupérer une liste de packages dans AWS Panorama	List			
ListPackages	Permet de récupérer une liste de packages dans AWS Panorama	List			
ListTagsForResource	Autorise la récupération d'une liste de balises pour une ressource dans AWS Panorama	Lecture	applicationInstance		
			device		
			package		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ProvisionDevice	Autorise l'enregistrement d'un appareil AWS Panorama	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterPackageVersion	Autorise l'enregistrement d'une version du package AWS Panorama	Écrire	package*		
RemoveApplicationInstance	Autorise la suppression d'une instance d'application AWS Panorama	Écrire	applicationInstance*		
SignalApplicationInstanceNodeInstances	Autorise les nœuds de caméra d'une instance d'application à faire une pause ou à reprendre	Écrire	applicationInstance*		
TagResource	Autorise l'ajout de balises à une ressource dans AWS Panorama	Identification	applicationInstance		
			device		
			package		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Autorise à supprimer les balises d'une ressource dans AWS Panorama	Identification	applicationInstance		
			device		
			package		
				aws:TagKeys	
UpdateDeviceMetadata	Autorise la modification des paramètres de base d'un appareil AWS Panorama	Écrire	device*		

Types de ressources définis par AWS Panorama

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
device	arn:${Partition}:panorama:${Region}:${Account}:device/${DeviceId}	aws:ResourceTag/${TagKey}
package	arn:${Partition}:panorama:${Region}:${Account}:package/${PackageId}	aws:ResourceTag/${TagKey}
applicationInstance	arn:${Partition}:panorama:${Region}:${Account}:applicationInstance/${ApplicationInstanceId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Panorama

AWS Panorama définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le service de calcul AWS parallèle

AWS Le service Parallel Computing (préfixe de service :`pcs`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Parallel Computing Service
- Types de ressources définis par AWS Parallel Computing Service
- Clés de condition pour le service de calcul AWS parallèle

Actions définies par AWS Parallel Computing Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource	Accorde l'autorisation de configurer la livraison des journaux vendus pour les journaux du cluster AWS PCS	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCluster	Accorde l'autorisation de créer des clusters	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:CreateSecret secretsmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateComputeNodeGroup	Accorde l'autorisation de créer des groupes de nœuds de calcul	Écrire	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunch

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					TemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Accorde l'autorisation de créer des files d'attente	Écrire	cluster*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Accorde l'autorisation de supprimer des clusters	Écrire	cluster*		ec2:DeleteNetworkInterface secretsmanager:DeleteSecret

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteComputeNodeGroup	Autorise la suppression de groupes de nœuds de calcul	Écrire	cluster*		ec2:DeleteLaunchTemplate ec2:TerminateInstances
			computenodegroup*		
DeleteQueue	Accorde l'autorisation de supprimer des files d'attente	Écrire	cluster*		
			queue*		
GetCluster	Accorde l'autorisation d'obtenir les propriétés du cluster	Lecture	cluster*		
GetComputeNodeGroup	Accorde l'autorisation d'obtenir les propriétés du groupe de nœuds de calcul	Lecture	cluster*		
			computenodegroup*		
GetQueue	Accorde l'autorisation d'obtenir les propriétés de la file d'attente	Lecture	cluster*		
			queue*		
ListClusters	Accorde l'autorisation de répertorier les clusters virtuels	List			
ListComputeNodeGroups	Accorde l'autorisation de répertorier les groupes de nœuds de calcul	List	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListQueues	Accorde l'autorisation de répertorier les files d'attente	List	cluster*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture			
RegisterComputeNodeGroupInstance	Accorde l'autorisation d'enregistrer une instance de calcul dans un groupe de nœuds de calcul	Écrire	cluster*		secretsmanager:GetSecretValue
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	cluster	aws:ResourceTag/${TagKey}	
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	cluster	aws:ResourceTag/${TagKey}	
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCluster	Accorde l'autorisation de mettre à jour les propriétés du cluster	Écrire	cluster*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:CreateSecret secretsmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateComputeNodeGroup	Autorise la mise à jour des propriétés du groupe de nœuds de calcul	Écrire	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunch

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					TemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole
			computenodegroup*		
UpdateQueue	Autorise la mise à jour des propriétés de la file d'attente	Écrire	cluster*		
			queue*		

Types de ressources définis par AWS Parallel Computing Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}`	aws:ResourceTag/${TagKey}
computenodegroup	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/computenodegroup/${ComputeNodeGroupIdentifier}`	aws:ResourceTag/${TagKey}
queue	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/queue/${QueueIdentifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour le service de calcul AWS parallèle

AWS Le service de calcul parallèle définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Partner Central

AWS Partner Central (préfixe de service :`partnercentral`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Partner Central
- Types de ressources définis par AWS Partner Central
- Clés de condition pour AWS Partner Central

Actions définies par AWS Partner Central

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptChannelHandshake	Autorise les chaînes à accepter les poignées de main dans Partner Central AWS	Écrire	ChannelHandshake*		
				partnercentral:Catalog partnercentral:ChannelHandshakeType	
AcceptConnectionInvitation	Autorise l'acceptation des invitations de connexion dans AWS Partner Central	Écrire	ConnectionInvitation*		
				partnercentral:Catalog	
AcceptEngagementInvitation	Autorise l'acceptation des invitations d'engagement sur AWS Partner Central	Écrire	engagement-invitation*		
				partnercentral:Catalog	
AmendBenefitApplication	Autorise la modification des demandes de prestations dans AWS Partner Central	Écrire	BenefitApplication*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
AssignOpportunity	Accorde l'autorisation d'attribuer des opportunités sur AWS Partner Central	Écrire	Opportunity*		
				partnercentral:Catalog	
AssociateAwsTrainingCertificationEmailDomain	Accorde l'autorisation d'associer AWS Training et de certifier des domaines de messagerie dans AWS Partner Central	Écrire	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate BenefitApplication Resource	Donne l'autorisation d'associer des ressources de demande d'avantages dans AWS Partner Central	Écrire	BenefitAllocation*		
			BenefitApplication*		
			Opportunity*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
Associate Opportunity	Permet d'associer des opportunités sur AWS Partner Central à d'autres entités	Écrire	Opportunity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				partnercentral:Catalog partnercentral:RelatedEntityType	
CancelBenefitApplication	Autorise l'annulation des demandes de prestations dans AWS Partner Central	Écrire	BenefitApplication*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
CancelChannelHandshake	Autorise l'annulation des poignées de main d'une chaîne dans Partner Central AWS	Écrire	ChannelHandshake*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:ChannelHandshakeType	
CancelConnection	Autorise l'annulation des connexions dans AWS Partner Central	Écrire	Connection*		
				partnercentral:Catalog	
CancelConnectionInvitation	Autorise l'annulation des invitations de connexion dans AWS Partner Central	Écrire	ConnectionInvitation*		
				partnercentral:Catalog	
CancelProfileUpdateTask	Autorise l'annulation des tâches de mise à jour du profil dans AWS Partner Central	Écrire	Partner*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
CreateBenefitApplication	Autorise la création de demandes de prestations dans AWS Partner Central	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBusinessPlan [autorisation uniquement]	Autorise la création de plans d'affaires dans AWS Partner Central	Écrire			
CreateChannelHandshake	Autorise la création de poignées de main pour les chaînes dans Partner Central AWS	Écrire	ProgramManagementAccount		
			Relationship		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:ChannelHandshakeType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCollaborationChannelMembers [autorisation uniquement]	Autorise la création de membres d'un canal de collaboration dans AWS Partner Central	Écrire			
CreateCollaborationChannelRequest [autorisation uniquement]	Autorise la création de demandes de canaux de collaboration dans AWS Partner Central	Écrire			
CreateConnectionInvitation	Accorde l'autorisation de créer des invitations de connexion dans AWS Partner Central	Écrire		partnercentral:Catalog	
CreateEngagement	Autorise la création d'engagements dans AWS Partner Central	Écrire	Engagement*		
				partnercentral:Catalog	
CreateEngagementContext	Autorise la création de contextes d'engagement dans AWS Partner Central	Écrire	Engagement*		
				partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEngagementInvitation	Autorise la création d'invitations à des engagements dans AWS Partner Central	Écrire	engagement-invitation*		
				partnercentral:Catalog	
CreateOpportunity	Autorise la création de nouvelles opportunités sur AWS Partner Central	Écrire	Opportunity*		
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePartner	Autorise la création de partenaires dans AWS Partner Central	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
CreateProgramManagementAccount	Autorise la création de comptes de gestion de programme dans AWS Partner Central	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
CreateRelationship	Autorise la création de relations dans AWS Partner Central	Écrire	ProgramManagementAccount*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
CreateResourceSnapshot	Autorise la création d'instantanés de ressources dans AWS Partner Central	Écrire	ResourceSnapshot*		
				partnercentral:Catalog	
CreateResourceSnapshotJob	Autorise la création de jobs de capture instantanée des ressources dans AWS Partner Central	Écrire	resource-snapshot-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	
DeleteProgramManagementAccount	Autorise la suppression des comptes de gestion du programme dans AWS Partner Central	Écrire	ProgramManagementAccount*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
DeleteRelationship	Autorise la suppression de relations dans AWS Partner Central	Écrire	Relationship*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteResourceSnapshotJob	Autorise la suppression des tâches liées aux instantanés des ressources sur AWS Partner Central	Écrire	resource-snapshot-job*		
				partnercentral:Catalog	
DisassociateAwsTrainingCertificationEmailDomain	Accorde l'autorisation de dissocier AWS Training et de certifier les domaines de messagerie dans AWS Partner Central	Écrire	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
DisassociateBenefitApplicationResource	Autorise la dissociation des ressources relatives aux demandes de prestations dans AWS Partner Central	Écrire	BenefitAllocation*		
			BenefitApplication*		
			Opportunity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
DisassociateOpportunity	Permet de dissocier les opportunités sur AWS Partner Central des autres entités	Écrire	Opportunity*		
				partnercentral:Catalog partnercentral:RelatedEntityType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnrollInPartnerPath [autorisation uniquement]	Accorde l'autorisation de s'inscrire à des parcours partenaires dans AWS Partner Central	Écrire			
GetAllianceLeadContact	Autorise la récupération des informations de contact du responsable de l'alliance dans AWS Partner Central	Lecture	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetAwsOpportunitySummary	Accorde l'autorisation de récupérer AWS les résumés des opportunités sur AWS Partner Central	Lecture	Opportunity*		
				partnercentral:Catalog	
GetBenefit	Autorise la récupération des informations relatives aux avantages dans AWS Partner Central	Lecture	Benefit*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
GetBenefitAllocation	Donne l'autorisation de récupérer les informations relatives à l'allocation des avantages dans AWS Partner Central	Lecture	BenefitAllocation*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBenefitApplication	Donne l'autorisation de récupérer les informations relatives à la demande de prestations dans AWS Partner Central	Lecture	BenefitApplication*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
GetBusinessPlan [autorisation uniquement]	Accorde l'autorisation de récupérer les détails du plan d'affaires dans AWS Partner Central	Lecture			
GetCollaborationChannel [autorisation uniquement]	Accorde l'autorisation de récupérer les détails du canal de collaboration dans AWS Partner Central	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConnection	Autorise la récupération des informations de connexion dans AWS Partner Central	Lecture	Connection*		
				partnercentral:Catalog	
GetConnectionInvitation	Accorde l'autorisation de récupérer les détails de l'invitation de connexion dans AWS Partner Central	Lecture	ConnectionInvitation*		
				partnercentral:Catalog	
GetConnectionPreferences	Autorise la récupération des préférences de connexion dans AWS Partner Central	Lecture		partnercentral:Catalog	
GetEngagement	Autorise la récupération des détails de l'engagement dans AWS Partner Central	Lecture	Engagement*		
				partnercentral:Catalog	
GetEngagementInvitation	Accorde l'autorisation de récupérer les détails des invitations d'engagement sur AWS Partner Central	Lecture	engagement-invitation*		
				partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetOpportunity	Donne l'autorisation de récupérer les détails des opportunités sur AWS Partner Central	Lecture	Opportunity*		
				partnercentral:Catalog	
GetPartner	Autorise la récupération des informations sur les partenaires dans AWS Partner Central	Lecture	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetPartnerDashboard	Autorise la récupération des informations du tableau de bord des AWS partenaires dans Partner Central	Lecture	Dashboard*		
				partnercentral:Catalog	
GetPartnerProfile [autorisation uniquement]	Autorise la récupération des informations du profil public du AWS partenaire dans Partner Central	Lecture			
GetProfileUpdateTask	Accorde l'autorisation de récupérer les détails des tâches de mise à jour du profil dans AWS Partner Central	Lecture	Partner*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetProfileVisibility	Autorise la récupération des paramètres de visibilité du profil dans AWS Partner Central	Lecture	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetProgramManagementAccount [autorisation uniquement]	Autorise la récupération des informations du compte de gestion du programme dans AWS Partner Central	Lecture		partnercentral:Catalog	
GetRelationship	Autorise la récupération des informations relatives à la relation dans AWS Partner Central	Lecture	Relationship*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetResourceSnapshot	Autorise la récupération des informations relatives aux instantanés des ressources dans AWS Partner Central	Lecture	ResourceSnapshot*		
				partnercentral:Catalog	
GetResourceSnapshotJob	Autorise la récupération des informations relatives à une tâche instantanée des ressources dans AWS Partner Central	Lecture	resource-snapshot-job*		
				partnercentral:Catalog	
GetSellingSystemSettings	Autorise la récupération des paramètres du système de vente dans AWS Partner Central	Lecture		partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetVerification	Autorise la récupération des informations de vérification dans AWS Partner Central	Lecture		partnercentral:Catalog partnercentral:VerificationType	
ListBenefitAllocations	Donne l'autorisation de répertorier les allocations d'avantages dans AWS Partner Central	List	BenefitAllocation*		
				partnercentral:Catalog partnercentral:FulfillmentTypes	
ListBenefitApplications	Donne l'autorisation de répertorier les demandes de prestations dans AWS Partner Central	List	BenefitApplication*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
ListBenefits	Donne l'autorisation de répertorier les avantages dans AWS Partner Central	List	Benefit*		
				partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
ListBusinessPlans [autorisation uniquement]	Permet de répertorier les plans d'affaires dans AWS Partner Central	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListChannelHandshakes	Permet de répertorier les poignées de main des chaînes dans Partner Central AWS	List	ChannelHandshake*		
				partnercentral:Catalog partnercentral:ChannelHandshakeType	
ListCollaborationChannels [autorisation uniquement]	Permet de répertorier les canaux de collaboration dans AWS Partner Central	List			
ListConnectionInvitations	Accorde l'autorisation de répertorier les invitations de connexion dans AWS Partner Central	List		partnercentral:Catalog	
ListConnections	Autorise à répertorier les connexions dans AWS Partner Central	List		partnercentral:Catalog	
ListEngagementByAcceptingInvitationTasks	Autorise à répertorier les engagements en acceptant les tâches d'invitation dans AWS Partner Central	List		partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEngagementFromOpportunityTasks	Autorise à répertorier les engagements issus des tâches d'opportunité dans AWS Partner Central	List		partnercentral:Catalog	
ListEngagementInvitations	Accorde l'autorisation de répertorier les invitations à des engagements sur AWS Partner Central	List		partnercentral:Catalog	
ListEngagementMembers	Permet de répertorier les membres de l'engagement dans AWS Partner Central	Lecture	Engagement*		
				partnercentral:Catalog	
ListEngagementResourceAssociations	Permet de répertorier les associations de ressources d'engagement dans AWS Partner Central	Lecture	ResourceSnapshot*		
				partnercentral:Catalog	
ListEngagements	Autorise à répertorier les engagements dans AWS Partner Central	List		partnercentral:Catalog	
ListOpportunities	Donne l'autorisation de répertorier les opportunités sur AWS Partner Central	List		partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOpportunityFromEngagementTasks	Permet de répertorier les opportunités issues des tâches d'engagement dans AWS Partner Central	List		partnercentral:Catalog	
ListPartnerPaths [autorisation uniquement]	Permet de répertorier les parcours des partenaires dans AWS Partner Central	List			
ListPartners	Accorde l'autorisation de répertorier les partenaires dans AWS Partner Central	List		partnercentral:Catalog	
ListProgramManagementAccounts	Permet de répertorier les comptes de gestion du programme dans AWS Partner Central	List	ProgramManagementAccount*		
				partnercentral:Catalog	
ListRelationships	Accorde l'autorisation de répertorier les relations dans AWS Partner Central	List	Relationship*		
				partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceSnapshotJobs	Autorise à répertorier les jobs relatifs à des instantanés de ressources dans AWS Partner Central	List		partnercentral:Catalog	
ListResourceSnapshots	Autorise à répertorier des instantanés de ressources dans AWS Partner Central	List	ResourceSnapshot*		
				partnercentral:Catalog	
ListSolutions	Autorise la mise en vente de solutions sur AWS Partner Central	List		partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation d'ajouter des balises de liste à une ressource. Ressource prise en charge : ResourceSnapshotJob	Lecture		aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
PutAllianceLeadContact	Autorise le responsable de l'alliance à définir les coordonnées du responsable de l'alliance dans AWS Partner Central	Écrire	Partner*	aws:ResourceTag/${TagKey} partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutBusinessPlan [autorisation uniquement]	Autorise la mise à jour des plans d'affaires dans AWS Partner Central	Écrire			
PutProfileVisibility	Accorde l'autorisation de définir la visibilité du profil dans AWS Partner Central	Écrire	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
PutSellingSystemSettings	Autorise l'installation des paramètres du système de vente dans AWS Partner Central	Écrire			
RecallBenefitApplication	Autorise le rappel des demandes de prestations dans AWS Partner Central	Écrire	BenefitApplication*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
RejectChannelHandshake	Autorise le rejet des poignées de main d'une chaîne dans Partner Central AWS	Écrire	ChannelHandshake*		
				partnercentral:Catalog partnercentral:ChannelHandshakeType	
RejectConnectionInvitation	Autorise le rejet des invitations de connexion dans AWS Partner Central	Écrire	ConnectionInvitation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				partnercentral:Catalog	
RejectEngagementInvitation	Autorise le rejet des invitations d'engagement sur AWS Partner Central	Écrire	engagement-invitation*		
				partnercentral:Catalog	
SearchPartnerProfiles [autorisation uniquement]	Autorise la recherche de profils publics de partenaires dans AWS Partner Central	List			
SendEmailVerificationCode	Autorise l'envoi de codes de vérification par e-mail dans AWS Partner Central	Écrire		partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartEngagementByAcceptingInvitationTask	Accorde l'autorisation de lancer des tâches qui démarrent des engagements sur AWS Partner Central en acceptant une invitation à un engagement	Écrire	engagement-by-accepting-invitation-task*		partnercentral:AcceptEngagementInvitation partnercentral:CreateOpportunity partnercentral:CreateResourceSnapshotJob partnercentral:GetEngagementInvitation partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartEngagementFromOpportunityTask	Accorde l'autorisation de lancer des tâches qui démarrent des engagements à partir d'opportunités sur AWS Partner Central	Écrire	engagement-from-opportunity-task*		partnercentral:CreateEngagement partnercentral:CreateEngagementInvitation partnercentral:CreateResourceSnapshotJob partnercentral:GetOpportunity partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartOpportunityFromEngagementTask	Accorde l'autorisation de lancer des tâches qui démarrent Opportunities from Engagements sur AWS Partner Central	Écrire	OpportunityFromEngagementTask*		partnercentral:CreateEngagementContext partnercentral:CreateOpportunity partnercentral:CreateResourceSnapshot partnercentral:CreateResourceSnapshotJob partnercentral:GetEngagement partnercentral:StartResourc

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					eSnapshotJob
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
StartProfileUpdateTask	Autorise le lancement de tâches de mise à jour du profil dans AWS Partner Central	Écrire	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
StartResourceSnapshotJob	Autorise le lancement de tâches de capture instantanée des ressources dans AWS Partner Central	Écrire	resource-snapshot-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				partnercentral:Catalog	
StartVerification	Autorise le lancement des processus de vérification dans AWS Partner Central	Écrire		partnercentral:Catalog partnercentral:VerificationType	
StopResourceSnapshotJob	Autorise l'arrêt des tâches liées aux instantanés des ressources dans AWS Partner Central	Écrire	resource-snapshot-job*		
				partnercentral:Catalog	
SubmitBenefitApplication	Donne l'autorisation de soumettre des demandes de prestations dans AWS Partner Central	Écrire	BenefitApplication*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
SubmitOpportunity	Donne l'autorisation de soumettre des opportunités sur AWS Partner Central	Écrire	Opportunity*		
				partnercentral:Catalog	
TagResource	Accorde l'autorisation d'ajouter de nouvelles balises à une ressource. Ressource prise en charge : ResourceSnapshotJob	Identification	BenefitApplication		
			ChannelHandshake		
			Opportunity		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Partner		
			ProgramManagementAccount		
			Relationship		
			resource-snapshot-job		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
UntagResource	Accorde l'autorisation de supprimer les balises d'une ressource. Ressource prise en charge : ResourceSnapshotJob	Identification	BenefitApplication		
			ChannelHandshake		
			Opportunity		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Partner		
			ProgramManagementAccount		
			Relationship		
			resource-snapshot-job		
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateBenefitApplication	Autorise la mise à jour des demandes de prestations dans AWS Partner Central	Écrire	BenefitApplication*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
UpdateConnectionPreferences	Autorise la mise à jour des préférences de connexion dans AWS Partner Central	Écrire		partnercentral:Catalog	
UpdateEngagementContext	Autorise la mise à jour des contextes d'engagement dans AWS Partner Central	Écrire	Engagement*		
				partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateOpportunity	Autorise la mise à jour des opportunités sur AWS Partner Central	Écrire	Opportunity*		
				partnercentral:Catalog	
UpdateProgramManagementAccount	Autorise la mise à jour des comptes de gestion du programme dans AWS Partner Central	Écrire	ProgramManagementAccount*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
UpdateRelationship	Autorise la mise à jour des relations dans AWS Partner Central	Écrire	Relationship*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UseSession [autorisation uniquement]	Autorise l'utilisation des sessions des agents Partner Central dans AWS Partner Central	Écrire		partnercentral:Catalog	

Types de ressources définis par AWS Partner Central

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Engagement	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement/${Identifier}`	
engagement-by-accepting-invitation-task	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-by-accepting-invitation-task/${TaskId}`	
engagement-from-opportunity-task	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-from-opportunity-task/${TaskId}`	

Types de ressources	ARN	Clés de condition
engagement-invitation	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-invitation/${Identifier}	
Opportunity	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/opportunity/${Identifier}	aws:ResourceTag/${TagKey}
resource-snapshot-job	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/resource-snapshot-job/${Identifier}	aws:ResourceTag/${TagKey}
ResourceSnapshot	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/engagement/${EngagementIdentifier}/resource/${ResourceType}/${ResourceIdentifier}/template/${TemplateIdentifier}/resource-snapshot/${SnapshotRevision}	
Solution	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/solution/${Identifier}	
Partner	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/partner/${Identifier}	aws:ResourceTag/${TagKey}
Connection	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/connection/${Identifier}	
ConnectionInvitation	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/connection-invitation/${Identifier}	

Types de ressources	ARN	Clés de condition
ConnectionPreferences	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/connection-preferences	
OpportunityFromEngagementTask	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/opportunity-from-engagement-task/${TaskId}	
Benefit	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/benefit/${Identifier}	
BenefitAllocation	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/benefit-allocation/${Identifier}	
BenefitApplication	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/benefit-application/${Identifier}	aws:ResourceTag/${TagKey}
ProgramManagementAccount	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/program-management-account/${Identifier}	aws:ResourceTag/${TagKey}
Relationship	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/program-management-account/${ProgramManagementAccountId}/relationship/${RelationshipId}	aws:ResourceTag/${TagKey}
ChannelHandshake	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/channel-handshake/${Identifier}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
Dashboard	`arn:${Partition}:partnercentral::${Account}:catalog/${Catalog}/ReportingData/${TableId}/Dashboard/${DashboardId}`	

Clés de condition pour AWS Partner Central

AWS Partner Central définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
partnercentral:Catalog	Filtre l'accès par un catalogue spécifique	String
partnercentral:ChannelHandshakeType	Filtre l'accès par type de poignée de main sur les chaînes	String

Clés de condition	Description	Type
partnercentral:FulfillmentTypes	Filtre l'accès par type de prestation des avantages	ArrayOfString
partnercentral:Programs	Filtre l'accès par programme	ArrayOfString
partnercentral:RelatedEntityType	Filtre l'accès par type d'entité pour Opportunity association	String
partnercentral:VerificationType	Filtre l'accès en fonction du type de vérification effectué	String

Actions, ressources et clés de condition pour la gestion centrale des comptes des AWS partenaires

AWS La gestion centrale des comptes des partenaires (préfixe de service :`partnercentral-account-management`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par la gestion centrale des comptes des AWS partenaires
- Types de ressources définis par la gestion centrale des comptes des AWS partenaires
- Clés de condition pour la gestion centrale des comptes des AWS partenaires

Actions définies par la gestion centrale des comptes des AWS partenaires

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AccessLegacyPartnerCentral [autorisation uniquement]	Autorise l'authentification unique de AWS Partner Central à Legacy Partner Central	Écrire		partnercentral-account-management:LegacyPartnerCentralRole	
AccessMarketingCentral [autorisation uniquement]	Autorise l'authentification unique depuis AWS Partner Central vers Marketing Central	Écrire		partnercentral-account-management:MarketingCentralRole	
AccessProServeTools [autorisation uniquement]	Autorise l'authentification unique depuis AWS Partner Central vers Tools ProServe	Écrire		partnercentral-account-management:ProServeRole	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociatePartnerAccount [autorisation uniquement]	Accorde l'autorisation d'associer un compte partenaire à Compte AWS	Écrire			
AssociatePartnerUser	Accorde l'autorisation pour associer l'utilisateur partenaire au rôle IAM	Écrire			
DisassociatePartnerUser	Accorde l'autorisation pour dissocier l'utilisateur partenaire du rôle IAM	Écrire			

Types de ressources définis par la gestion centrale des comptes des AWS partenaires

AWS La gestion centrale des comptes des partenaires ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à la gestion des comptes AWS Partner centraux, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour la gestion centrale des comptes des AWS partenaires

AWS La gestion centrale des comptes des partenaires définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
partnercentral-account-management:LegacyPartnerCentralRole	Filtre l'accès en fonction du rôle Legacy Partner Central	ArrayOfString
partnercentral-account-management:MarketingCentralRole	Filtre l'accès par rôle dans Marketing Central	ArrayOfString
partnercentral-account-management:ProServeRole	Filtre l'accès par rôle dans ProServe les outils	ArrayOfString

Actions, ressources et clés de condition pour la cryptographie des AWS paiements

AWS La cryptographie des paiements (préfixe de service :`payment-cryptography`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par la cryptographie des AWS paiements
- Types de ressources définis par la cryptographie des AWS paiements

- Clés de condition pour la cryptographie des AWS paiements

Actions définies par la cryptographie des AWS paiements

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddKeyReplicationRegions	Autorise l'ajout de régions de réplication à une clé de cryptographie AWS de paiement existante	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
CreateAlias	Accorde l'autorisation de créer un nom convivial pour une clé	Écrire	alias*		
			key*		
CreateKey	Accorde l'autorisation de créer une clé unique gérée par le client dans la région Compte AWS et dans la région de l'appelant	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	payment-cryptography:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				payment-cryptography:KeyClass payment-cryptography:KeyUsage payment-cryptography:KeyAlgorithm	
DecryptData	Accorde l'autorisation de déchiffrer les données de type texte chiffré à l'aide d'une clé de chiffrement des données symétrique, asymétrique ou DUKPT	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
DeleteAlias	Accorde l'autorisation de supprimer l'alias de spécifié	Écrire	alias*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteKey	Accorde l'autorisation de planifier la suppression d'une clé	Écrire	key*		
				payment-cryptography:RequestAlias	
DisableDefaultKeyReplicationRegions	Accorde l'autorisation de désactiver les régions de réplication clés par défaut pour la réplication au niveau du compte	Écrire			
EnableDefaultKeyReplicationRegions	Accorde l'autorisation d'activer les régions de réplication clés par défaut pour la réplication au niveau du compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EncryptData	Accorde l'autorisation de chiffrer les données de type texte clair en texte chiffré à l'aide d'une clé de chiffrement des données symétrique, asymétrique ou DUKPT	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
ExportKey	Accorde l'autorisation d'exporter une clé à partir du service	Écrire	key*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				payment-cryptography:RequestAlias payment-cryptography:CertificateAuthorityPublicKeyIdentifier payment-cryptography:WrappingKeyIdentifier	
GenerateAs2805KekValidation	Accorde l'autorisation de générer un KekValidationRequest ou un KekValidationResponse pour l' node-to-nodeinitialisation entre les nœuds de traitement des paiements à l'aide de la norme australienne 2805 () AS2805	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GenerateCardValidationData	Autorise la génération de données relatives aux cartes à l'aide d'algorithmes tels que les valeurs de vérification des cartes (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) ou les codes de sécurité des cartes (CSC) qui vérifient la validité d'une carte à bande magnétique	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
GenerateMac	Accorde l'autorisation de générer un cryptogramme MAC (Message Authentication Code, Code d'authentification de message)	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
GenerateMacEmvPinChange	Accorde l'autorisation de générer un cryptogramme MAC (Message Authentication Code, Code d'authentification de message)	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GeneratePinData	Accorde l'autorisation de générer des données relatives au code PIN, telles que le code PIN, la valeur de vérification du code PIN (PVV), le blocage du code PIN et le décalage du code PIN, lors de l'émission ou de la réémission d'une nouvelle carte	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
GetAlias	Accorde l'autorisation de renvoyer le keyArn associé à un aliasName	Lecture	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCertificateSigningRequest	Accorde l'autorisation de renvoyer la demande de signature de certificat pour une clé publique à partir d'une clé de classe PUBLIC_KEY	Lecture	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDefaultKeyReplicationRegions	Accorde l'autorisation de récupérer les régions de réplication clés par défaut configurées au niveau du compte	Lecture			
GetKey	Accorde l'autorisation de renvoyer les informations détaillées concernant la clé spécifiée	Lecture	key*		
				payment-cryptography:RequestAlias	
GetParametersForExport	Accorde l'autorisation d'obtenir le jeton d'exportation et le certificat de la clé de signature pour lancer une exportation de clé TR-34	Lecture			
GetParametersForImport	Accorde l'autorisation d'obtenir le jeton d'importation et le certificat de la clé d'encapsulage pour lancer une importation de clé TR-34	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPublicKeyCertificate	Accorde l'autorisation de renvoyer la clé publique à partir d'une clé de la classe PUBLIC_KEY	Lecture	key*		
				payment-cryptography:RequestAlias	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportKey	Accorde l'autorisation d'importer des clés et des certificats de clé publique	Écrire		aws:RequestTag/${TagKey} aws:TagKeys payment-cryptography:ImportKeyMaterial payment-cryptography:CertificateAuthorityPublicKeyIdentifier payment-cryptography:WrappingKeyIdentifier	payment-cryptography:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAliases	Accorde l'autorisation de renvoyer une liste d'alias créée pour toutes les clés de l'appelant et de Compte AWS la région	List			
ListKeys	Accorde l'autorisation de renvoyer une liste de clés créée dans la région Compte AWS et dans la région de l'appelant	List			
ListTagsForResource	Accorde l'autorisation de renvoyer une liste de tags créés dans la région Compte AWS et dans la région de l'appelant	Lecture	key		
ReEncryptData	Accorde l'autorisation de rechiffrer le texte chiffré à l'aide de clés de chiffrement des données DUKPT, symétriques et asymétriques	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
RemoveKeyReplicationRegions	Autorise la suppression de régions de réplication d'une clé de cryptographie AWS de paiement existante	Écrire	alias*		
			key*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				payment-cryptography:RequestAlias	
RestoreKey	Accorde l'autorisation d'annuler la suppression d'une clé planifiée si, à un moment quelconque de la période d'attente, une clé doit être réactivée	Écrire	key*		
				payment-cryptography:RequestAlias	
StartKeyUsage	Accorde l'autorisation d'activer une clé désactivée	Écrire	key*		
				payment-cryptography:RequestAlias	
StopKeyUsage	Accorde l'autorisation de désactiver une clé activée	Écrire	key*		
				payment-cryptography:RequestAlias	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter ou d'écraser une ou plusieurs balises pour la ressource spécifiée	Identification	key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TranslateKeyMaterial	Accorde l'autorisation de traduire le type de clé encapsulée pour une clé encapsulée	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
TranslatePinData	Accorde l'autorisation de traduire un bloc PIN chiffré depuis et vers les formats ISO 9564 0,1,3,4	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
UntagResource	Accorde l'autorisation de supprimer la ou les balises spécifiées de la ressource spécifiée	Identification	key*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAlias	Accorde l'autorisation de modifier la clé à laquelle un alias est affecté ou d'annuler l'affectation de l'alias à sa clé actuelle	Écrire	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyAuthRequestCryptogram	Accorde l'autorisation de vérifier le cryptogramme de demande d'autorisation (ARQC) pour l'autorisation d'une carte de paiement à puce EMV	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
VerifyCardValidationData	Autorise la vérification des données de validation relatives aux cartes à l'aide d'algorithmes tels que les valeurs de vérification des cartes (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) et les codes de sécurité des cartes (CSC)	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
VerifyMac	Accorde l'autorisation de vérifier le MAC (Message Authentication Code, Code d'authentification de message) des données d'entrée par rapport à un MAC fourni	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	
VerifyPinData	Autorise la vérification des données relatives au code PIN, telles que le code PIN et le décalage du code PIN, à l'aide d'algorithmes tels que VISA PVV et IBM3624	Écrire	alias*		
			key*		
				payment-cryptography:RequestAlias	

Types de ressources définis par la cryptographie des AWS paiements

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
key	arn:${Partition}:payment-cryptography:${Region}:${Account}:key/${KeyId}	aws:ResourceTag/${TagKey} payment-cryptography:ResourceAliases
alias	arn:${Partition}:payment-cryptography:${Region}:${Account}:alias/${Alias}	payment-cryptography:ResourceAliases

Clés de condition pour la cryptographie des AWS paiements

AWS La cryptographie des paiements définit les clés de condition suivantes qui peuvent être utilisées dans le cadre `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et de la valeur de la balise contenue dans la demande pour l'opération spécifiée	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises affectées à une clé pour l'opération spécifiée	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise contenues dans la demande pour l'opération spécifiée	ArrayOfString

Clés de condition	Description	Type
payment-cryptography:CertificateAuthorityPublicKeyIdentifier	Filtre l'accès en fonction des informations CertificateAuthorityPublicKeyIdentifier spécifiées dans la demande ou dans ImportKey les ExportKey opérations et	String
payment-cryptography:ImportKeyMaterial	Filtre l'accès en fonction du type de matériau clé importé [RootCertificatePublicKey,, Tr34 TrustedCertificatePublicKey, Tr31KeyBlock, DiffieHellmanTr 31 KeyBlockKeyBlock, As2805KeyCryptogram] pour l'opération ImportKey	String
payment-cryptography:KeyAlgorithm	Filtre l'accès en KeyAlgorithm fonction des informations spécifiées dans la demande d' CreateKey opération	String
payment-cryptography:KeyClass	Filtre l'accès en KeyClass fonction des informations spécifiées dans la demande d' CreateKey opération	String
payment-cryptography:KeyUsage	Filtre l'accès en KeyClass fonction des informations spécifiées dans la demande ou associées à une clé pour l' CreateKey opération	String
payment-cryptography:RequestAlias	Filtre l'accès en fonction des alias contenus dans la demande pour l'opération spécifiée	String
payment-cryptography:ResourceAliases	Filtre l'accès en fonction des alias associés à une clé pour l'opération spécifiée	ArrayOfString

Clés de condition	Description	Type
payment-cryptography:WrappingKeyIdentifier	Filtre l'accès en fonction des informations WrappingKeyIdentifier spécifiées dans la demande pour ImportKey les ExportKey opérations et	String

Actions, ressources et clés de condition pour les AWS paiements

AWS Payments (préfixe de service :`payments`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Payments
- Types de ressources définis par AWS Payments
- Clés de condition pour les AWS paiements

Actions définies par AWS Payments

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptFinancingApplicationTerms	Donne l'autorisation d'accepter les conditions d'une demande de financement fournies par un prêteur	Écrire			
CreateFinancingApplication	Donne l'autorisation de créer une demande de financement	Écrire			
CreatePaymentInstrument	Accorde l'autorisation de créer un instrument de paiement	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
DeletePaymentInstrument [autorisation uniquement]	Accorde l'autorisation de supprimer un instrument de paiement	Écrire			
GetFinancingApplication	Donne l'autorisation d'obtenir des informations sur une demande de financement	Lecture			
GetFinancingLine	Donne l'autorisation d'obtenir des informations sur une ligne de financement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFinancingLineWithdrawal	Donne l'autorisation d'obtenir des informations sur le retrait d'une ligne de financement	Lecture			
GetFinancingOption	Donne l'autorisation d'obtenir des informations sur une option de financement	Lecture			
GetPaymentInstrument	Accorde l'autorisation d'obtenir des informations sur un instrument de paiement	List	payment-instrument		
GetPaymentStatus [autorisation uniquement]	Accorde l'autorisation d'obtenir le statut de paiement de factures	Lecture			
ListFinancingApplications	Accorde l'autorisation de répertorier les métadonnées des demandes de financement	List			
ListFinancingLineWithdrawals	Accorde l'autorisation de répertorier les métadonnées des retraits sur les lignes de financement	List			
ListFinancingLines	Accorde l'autorisation de répertorier les métadonnées des lignes de financement	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPaymentInstruments [autorisation uniquement]	Accorde l'autorisation de répertorier les métadonnées des instruments de paiement	List			
ListPaymentPreferences [autorisation uniquement]	Accorde l'autorisation d'obtenir les préférences de paiement (devise de paiement préférée, mode de paiement préféré, etc.)	List			
ListPaymentProgramOptions	Accorde l'autorisation de répertorier des informations sur les options de paiement	List			
ListPaymentProgramStatus	Accorde l'autorisation de répertorier des informations sur l'éligibilité au programme de paiement et le statut d'inscription	List			
ListTagsForResource	Accorde l'autorisation de répertorier des balises sur une ressource de paiement	List	payment-instrument		
MakePayment [autorisation uniquement]	Accorde l'autorisation d'effectuer un paiement, à authentifier un paiement, à vérifier un mode de paiement et à générer un document de demande de financement pour Advance Pay	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser une ressource de paiement	Identification	payment-instrument		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource de paiement	Identification	payment-instrument		
				aws:TagKeys	
UpdateFinancingApplication	Autorise la mise à jour d'une demande de financement	Écrire			
UpdatePaymentInstrument [autorisation uniquement]	Autorise la mise à jour d'un instrument de paiement	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePaymentPreferences [autorisation uniquement]	Accorde l'autorisation de mettre à jour les préférences de paiement (devise de paiement préférée, mode de paiement préféré, etc.)	Écrire			

Types de ressources définis par AWS Payments

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
payment-instrument	`arn:${Partition}:payments::${Account}:payment-instrument:${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les AWS paiements

AWS Payments définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Performance Insights

AWS Performance Insights (préfixe de service :`pi`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Performance Insights
- Types de ressources définis par AWS Performance Insights
- Clés de condition pour AWS Performance Insights

Actions définies par AWS Performance Insights

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePerformanceAnalysisReport	Accorde l'autorisation d'appeler CreatePerformanceAnalysisReport l'API pour créer un rapport d'analyse des performances pour une instance de base de données spécifiée	Écrire	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePerformanceAnalysisReport	Accorde l'autorisation d'appeler DeletePerformanceAnalysisReport l'API pour supprimer un rapport d'analyse des performances pour une instance de base de données spécifiée	Écrire	perf-reports-resource*		
DescribeDimensionKeys	Accorde l'autorisation d'appeler l' DescribeDimensionKeys API pour récupérer les clés de N principales dimensions d'une métrique pendant une période spécifique	Lecture	metric-resource*		
				pi:Dimensions	
GetDimensionKeyDetails	Accorde l'autorisation d'appeler GetDimensionKeyDetails l'API pour	Lecture	metric-resource*		
				pi:Dimensions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	récupérer les attributs du groupe de dimensions spécifié				
GetPerformanceAnalysisReport	Accorde l'autorisation d'appeler GetPerformanceAnalysisReport l'API pour récupérer un rapport d'analyse des performances pour une instance de base de données spécifiée	Lecture	perf-reports-resource*		
GetResourceMetadata	Accorde l'autorisation d'appeler GetResourceMetadata l'API pour récupérer les métadonnées des différentes fonctionnalités	Lecture	metric-resource*		
GetResourceMetrics	Accorde l'autorisation d'appeler GetResourceMetrics l'API pour récupérer les métriques PI pour un ensemble de sources de données, sur une période donnée	Lecture	metric-resource*		
				pi:Dimensions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAvailableResourceDimensions	Accorde l'autorisation d'appeler ListAvailableResourceDimensions l'API pour récupérer les dimensions qui peuvent être demandées pour chaque type de métrique spécifié sur une instance de base de données spécifiée	Lecture	metric-resource*		
ListAvailableResourceMetrics	Accorde l'autorisation d'appeler ListAvailableResourceMetrics l'API pour récupérer des métriques des types spécifiés qui peuvent être demandées pour une instance de base de données spécifiée	Lecture	metric-resource*		
ListPerformanceAnalysisReports	Accorde l'autorisation d'appeler ListPerformanceAnalysisReports l'API pour répertorier les rapports d'analyse des performances pour une instance de base de données spécifiée	List	perf-reports-resource*		
ListTagsForResource	Accorde l'autorisation d'appeler ListTagsForResource l'API pour répertorier les balises d'une ressource	List	metric-resource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			perf-reports-resource*		
TagResource	Accorde l'autorisation d'appeler TagResource l'API pour étiqueter une ressource	Identification	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'appeler UntagResource l'API pour annuler le balisage d'une ressource	Identification	perf-reports-resource*		
				aws:TagKeys	

Types de ressources définis par AWS Performance Insights

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
metric-resource	`arn:${Partition}:pi:${Region}:${Account}:metrics/${ServiceType}/${Identifier}`	aws:ResourceTag/${TagKey}
perf-reports-resource	`arn:${Partition}:pi:${Region}:${Account}:perf-reports/${ServiceType}/${Identifier}/${ReportId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Performance Insights

AWS Performance Insights définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
pi:Dimensions	Filtre l'accès selon les dimensions demandées	ArrayOfString

Actions, ressources et clés de condition pour Amazon Personalize

Amazon Personalize (préfixe de service : `personalize`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définie par Amazon Personalize
- Types de ressources définis par Amazon Personalize
- Clés de condition pour Amazon Personalize

Actions définie par Amazon Personalize

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBatchInferenceJob	Accorde l'autorisation de créer une tâche d'inférence par lots	Écrire	batchInferenceJob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBatchSegmentJob	Accorde l'autorisation de créer une tâche de segmentation par lots	Écrire	batchSegmentJob*		
CreateCampaign	Accorde l'autorisation de créer une campagne	Écrire	campaign*		
CreateDataDeletionJob	Accorde l'autorisation de créer une tâche de suppression de données	Écrire	dataDeletionJob*		
CreateDataInsightsJob	Accorde l'autorisation de créer une tâche d'analyse des données	Écrire	dataInsightsJob*		
CreateDataset	Accorde l'autorisation de créer un jeu de données.	Écrire	dataset*		
CreateDatasetExportJob	Accorde l'autorisation de créer une tâche d'exportation d'un jeu de données	Écrire	datasetExportJob*		
CreateDatasetGroup	Accorde l'autorisation de créer un groupe de jeux de données.	Écriture	datasetGroup*		
CreateDatasetImportJob	Accorde l'autorisation de créer une tâche d'importation d'un jeu de données.	Écriture	datasetImportJob*		
CreateEventTracker	Accorde l'autorisation de créer un dispositif de suivi d'événements	Écriture	eventTracker*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFilter	Accorde l'autorisation de créer un filtre	Écrire	filter*		
CreateMetricAttribution	Accorde l'autorisation de créer une annexe TGW RTB	Écrire	metricAttribution*		
CreateRecommender	Accorde l'autorisation de créer un système de recommandation	Écrire	recommender*		
CreateSchema	Accorde l'autorisation de créer un schéma	Écriture	schema*		
CreateSolution	Accorde l'autorisation de créer une solution	Écriture	solution*		
CreateSolutionVersion	Accorde l'autorisation de créer une version de solution	Écriture	solution*		
DeleteCampaign	Accorde l'autorisation de supprimer une campagne	Écriture	campaign*		
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données.	Écriture	dataset*		
DeleteDatasetGroup	Accorde l'autorisation de supprimer un groupe de jeux de données.	Écriture	datasetGroup*		
DeleteEventTracker	Accorde l'autorisation de supprimer un dispositif de suivi d'événements	Écriture	eventTracker*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFilter	Accorde l'autorisation de supprimer un filtre	Écrire	filter*		
DeleteMetricAttribution	Accorde l'autorisation de supprimer l'attribution d'une métrique	Écrire	metricAttribution*		
DeleteRecommender	Accorde l'autorisation de supprimer un système de recommandation	Écrire	recommender*		
DeleteSchema	Accorde l'autorisation de supprimer un schéma	Écriture	schema*		
DeleteSolution	Accorde l'autorisation de supprimer une solution, y compris toutes les versions de celle-ci.	Écriture	solution*		
DescribeAlgorithm	Accorde l'autorisation de décrire un algorithme	Lecture	algorithm*		
DescribeBatchInferenceJob	Accorde l'autorisation de décrire une tâche d'inférence par lots	Lecture	batchInferenceJob*		
DescribeBatchSegmentJob	Accorde l'autorisation de décrire une tâche de segmentation par lots	Lecture	batchSegmentJob*		
DescribeCampaign	Accorde l'autorisation de décrire une campagne	Lecture	campaign*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDataDeletionJob	Accorde l'autorisation de décrire une tâche de suppression de données	Lecture	dataDeletionJob*		
DescribeDataInsightsJob	Accorde l'autorisation de décrire une tâche d'analyse des données	Lecture	dataInsightsJob*		
DescribeDataset	Accorde l'autorisation de décrire un jeu de données.	Lecture	dataset*		
DescribeDatasetExportJob	Accorde l'autorisation de décrire une tâche d'exportation d'un jeu de données	Lecture	datasetExportJob*		
DescribeDatasetGroup	Accorde l'autorisation de décrire un groupe de jeux de données.	Lecture	datasetGroup*		
DescribeDatasetImportJob	Accorde l'autorisation de décrire une tâche d'importation d'un jeu de données.	Lecture	datasetImportJob*		
DescribeEventTracker	Accorde l'autorisation de décrire un dispositif de suivi d'événements	Lecture	eventTracker*		
DescribeFeatureTransformation	Accorde l'autorisation de décrire une transformation de fonction	Lecture	featureTransformation*		
DescribeFilter	Accorde l'autorisation de décrire un filtre	Lecture	filter*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeMetricAttribution	Accorde l'autorisation de décrire un attribut d'un VPC.	Lecture	metricAttribution*		
DescribeRecipe	Accorde l'autorisation de décrire une recette	Lecture	recipe*		
DescribeRecommender	Accorde l'autorisation de décrire un système de recommandation	Lecture	recommender*		
DescribeSchema	Accorde l'autorisation de décrire un schéma	Lecture	schema*		
DescribeSolution	Accorde l'autorisation de décrire une solution	Lecture	solution*		
DescribeSolutionVersion	Accorde l'autorisation de décrire une version d'une solution	Lecture	solution*		
GetActionRecommendations	Octroie l'autorisation d'obtenir une liste d'actions recommandées.	Lecture	campaign*		
GetDataInsights	Accorde l'autorisation d'obtenir des informations sur les données à partir d'une tâche d'analyse des données	Lecture	dataInsightsJob*		
GetPersonalizedRanking	Accorde l'autorisation d'obtenir une nouvelle liste classant les recommandations	Lecture	campaign*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRecommendations	Accorde l'autorisation d'obtenir une liste de recommandations à partir d'une campagne	Lecture	campaign*		
GetSolutionMetrics	Accorde l'autorisation d'obtenir des métriques pour une version de solution	Lecture	solution*		
ListBatchInferenceJobs	Accorde l'autorisation de répertorier des tâches d'inférence par lots	List			
ListBatchSegmentJobs	Accorde l'autorisation de répertorier des tâches de segmentation par lots	List			
ListCampaigns	Accorde l'autorisation de répertorier des campagnes	List			
ListDataDeletionJobs	Accorde l'autorisation de répertorier les tâches de suppression de données	List			
ListDataInsightsJobs	Accorde l'autorisation de répertorier les tâches d'analyse des données	List			
ListDatasetExportJobs	Accorde l'autorisation de répertorier les tâches d'exportation de jeu de données	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDatasetGroups	Accorde l'autorisation de répertorier des groupes de jeux de données	Liste			
ListDatasetImportJobs	Accorde l'autorisation de répertorier des tâches d'importation de jeu de données	Liste			
ListDatasets	Accorde l'autorisation de répertorier des jeux de données	Liste			
ListEventTrackers	Accorde l'autorisation de répertorier des dispositifs de suivi d'événements	Liste			
ListFilters	Accorde l'autorisation de répertorier des filtres	List			
ListMetricAttributionMetrics	Accorde l'autorisation de répertorier les métriques	List			
ListMetricAttributions	Accorde l'autorisation de répertorier les attributs de métriques	List			
ListRecipes	Accorde l'autorisation de répertorier des recettes	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRecommenders	Accorde l'autorisation de répertorier les systèmes de recommandation	List			
ListSchemas	Accorde l'autorisation de répertorier des schémas	Liste			
ListSolutionVersions	Accorde l'autorisation de répertorier des versions d'une solution	Liste			
ListSolutions	Accorde l'autorisation de répertorier des solutions	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource.	List			
PutActionInteractions	Octroie l'autorisation de saisir des données d'interaction d'action en temps réel.	Écrire			
PutActions	Octroie l'autorisation d'ingérer des données d'actions.	Écrire	dataset*		
PutEvents	Accorde l'autorisation de placer des données d'événement en temps réel	Écriture			
PutItems	Accorde l'autorisation d'ingérer des données Items	Écriture	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutUsers	Accorde l'autorisation d'ingérer des données Users	Écrire	dataset*		
StartRecommender	Accorde l'autorisation de démarrer un système de recommandation	Écrire	recommender*		
StopRecommender	Accorde l'autorisation d'arrêter un système de recommandation	Écrire	recommender*		
StopSolutionVersionCreation	Accorde l'autorisation d'arrêter la création d'une version de solution	Écrire	solution*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage			
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification			
UpdateCampaign	Accorde l'autorisation de mettre à jour une campagne	Écrire	campaign*		
UpdateDataset	Accorde l'autorisation de mettre à jour un jeu de données.	Écrire	dataset*		
UpdateMetricAttribution	Accorde l'autorisation de mettre à jour une métrique de parc	Écrire	metricAttribution*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRecommender	Accorde l'autorisation de mettre à jour un système de recommandation	Écrire	recommender*		
UpdateSolution	Autorise la mise à jour d'une solution	Écrire	solution*		

Types de ressources définis par Amazon Personalize

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
schema	`arn:${Partition}:personalize:${Region}:${Account}:schema/${ResourceId}`	
featureTransformation	`arn:${Partition}:personalize:::feature-transformation/${ResourceId}`	
dataset	`arn:${Partition}:personalize:${Region}:${Account}:dataset/${ResourceId}`	
datasetGroup	`arn:${Partition}:personalize:${Region}:${Account}:dataset-group/${ResourceId}`	

Types de ressources	ARN	Clés de condition
datasetImportJob	arn:${Partition}:personalize:${Region}:${Account}:dataset-import-job/${ResourceId}	
dataInsightsJob	arn:${Partition}:personalize:${Region}:${Account}:data-insights-job/${ResourceId}	
datasetExportJob	arn:${Partition}:personalize:${Region}:${Account}:dataset-export-job/${ResourceId}	
dataDeletionJob	arn:${Partition}:personalize:${Region}:${Account}:data-deletion-job/${ResourceId}	
solution	arn:${Partition}:personalize:${Region}:${Account}:solution/${ResourceId}	
campaign	arn:${Partition}:personalize:${Region}:${Account}:campaign/${ResourceId}	
eventTracker	arn:${Partition}:personalize:${Region}:${Account}:event-tracker/${ResourceId}	
recipe	arn:${Partition}:personalize:::recipe/${ResourceId}	
algorithm	arn:${Partition}:personalize:::algorithm/${ResourceId}	
batchInferenceJob	arn:${Partition}:personalize:${Region}:${Account}:batch-inference-job/${ResourceId}	

Types de ressources	ARN	Clés de condition
filter	`arn:${Partition}:personalize:${Region}:${Account}:filter/${ResourceId}`	
recommender	`arn:${Partition}:personalize:${Region}:${Account}:recommender/${ResourceId}`	
batchSegmentJob	`arn:${Partition}:personalize:${Region}:${Account}:batch-segment-job/${ResourceId}`	
metricAttribution	`arn:${Partition}:personalize:${Region}:${Account}:metric-attribution/${ResourceId}`	

Clés de condition pour Amazon Personalize

Personalize ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Pinpoint

Amazon Pinpoint (préfixe de service : `mobiletargeting`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Pinpoint
- Types de ressources définis par Amazon Pinpoint
- Clés de condition pour Amazon Pinpoint

Actions définies par Amazon Pinpoint

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApp	Accorde l'autorisation de créer une application	Écrire	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateCampaign	Accorde l'autorisation de créer une campagne pour une application	Écrire	app*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Accorde l'autorisation de créer un modèle d'e-mail	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateExportJob	Accorde l'autorisation de créer une tâche d'exportation qui exporte les définitions de point de terminaison vers Amazon S3.	Écrire	app*		
CreateImportJob	Accorde l'autorisation d'importer les définitions de point de terminaison pour créer un segment.	Écrire	app*		
CreateInAppTemplate	Accorde l'autorisation de créer un modèle de message in-app	Écrire	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateJourney	Accorde l'autorisation de créer un parcours pour une application	Écrire	journeys*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreatePushTemplate	Accorde l'autorisation de créer un modèle de notification push	Écrire	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecommenderConfiguration	Accorde l'autorisation de créer une configuration Amazon Pinpoint pour un modèle de recommandation.	Écrire	recommenders*		
CreateSegment	Accorde l'autorisation de créer un segment qui est basé sur les données de point de terminaison rapportées à Pinpoint par votre application. Pour permettre à un utilisateur de créer un segment en important des données de point de terminaison depuis l'extérieur de Pinpoint, autorisez l'action mobiletargeting : CreateImportJob	Écrire	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateSmsTemplate	Accorde l'autorisation de créer un modèle de message SMS	Écrire	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateVoiceTemplate	Accorde l'autorisation de créer un modèle de message vocal	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAdmChannel	Accorde l'autorisation de supprimer le canal ADM d'une application	Écrire	channel*		
DeleteApnsChannel	Accorde l'autorisation de supprimer la APNs chaîne pour une application	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteApnsSandboxChannel	Accorde l'autorisation de supprimer le canal APNs sandbox d'une application	Écrire	channel*		
DeleteApnsVoipChannel	Accorde l'autorisation de supprimer le canal APNs VoIP d'une application	Écrire	channel*		
DeleteApnsVoipSandboxChannel	Accorde l'autorisation de supprimer le canal sandbox APNs VoIP d'une application	Écrire	channel*		
DeleteApp	Accorde l'autorisation de supprimer une campagne spécifique	Écrire	app*		
DeleteBaiduChannel	Accorde l'autorisation de supprimer le canal Baidu d'une application	Écrire	channel*		
DeleteCampaign	Accorde l'autorisation de supprimer une campagne spécifique	Écrire	campaign*		
DeleteEmailChannel	Accorde l'autorisation de supprimer le canal de messagerie électronique d'une application	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEmailTemplate	Accorde l'autorisation de supprimer un modèle d'e-mail ou une version de modèle d'e-mail.	Écrire	template*		
DeleteEndpoint	Accorde l'autorisation de supprimer un point de terminaison	Écrire	endpoint*		
DeleteEventStream	Accorde l'autorisation de supprimer le flux d'événements d'une application	Écrire	event-stream*		
DeleteGcmChannel	Accorde l'autorisation de supprimer le canal GCM d'une application	Écrire	channel*		
DeleteInAppTemplate	Accorde l'autorisation de supprimer un modèle de message in-app ou une version de modèle de message in-app	Écrire	template*		
DeleteJourney	Accorde l'autorisation de supprimer un parcours spécifique	Écrire	journey*		
DeletePushTemplate	Accorde l'autorisation de supprimer un modèle de notification push ou une version de modèle de notification push.	Écrire	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRecommenderConfiguration	Accorde l'autorisation de supprimer une configuration Amazon Pinpoint pour un modèle de recommandation.	Écrire	recommender*		
DeleteSegment	Accorde l'autorisation de supprimer un segment spécifique	Écrire	segment*		
DeleteSmsChannel	Accorde l'autorisation de supprimer le canal SMS d'une application	Écrire	channel*		
DeleteSmsTemplate	Accorde l'autorisation de supprimer un modèle de message SMS ou une version de modèle de message SMS.	Écrire	template*		
DeleteUserEndpoints	Accorde l'autorisation de supprimer tous les points de terminaison qui sont associés à un ID d'utilisateur.	Écrire	user*		
DeleteVoiceChannel	Accorde l'autorisation de supprimer le canal vocal d'une application	Écrire	channel*		
DeleteVoiceTemplate	Accorde l'autorisation de supprimer un modèle de message vocal ou une version de modèle de message vocal.	Écrire	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAdmChannel	Accorde l'autorisation de récupérer des informations sur le canal Amazon Device Messaging (ADM) pour une application.	Lecture	channel*		
GetApnsChannel	Accorde l'autorisation de récupérer des informations sur le APNs canal pour une application	Lecture	channel*		
GetApnsSandboxChannel	Accorde l'autorisation de récupérer des informations sur le canal APNs sandbox d'une application	Lecture	channel*		
GetApnsVoipChannel	Accorde l'autorisation de récupérer des informations sur le canal APNs VoIP d'une application	Lecture	channel*		
GetApnsVoipSandboxChannel	Autorise une application à récupérer des informations sur le canal sandbox APNs VoIP	Lecture	channel*		
GetApp	Accorde l'autorisation de récupérer des informations sur une application spécifique dans votre compte Amazon Pinpoint.	Lecture	app*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetApplicationDateRangeKpi	Accorde l'autorisation de récupérer (requêtes) des données pré-agrégées pour fournir une métrique standard qui s'applique à une application.	Lecture	application-metrics*		
GetApplicationSettings	Accorde l'autorisation de récupérer les paramètres par défaut pour une application	List	app*		
GetApps	Accorde l'autorisation de récupérer une liste d'applications dans votre compte Amazon Pinpoint.	Lecture	apps*		
GetBaiduChannel	Accorde l'autorisation de récupérer des informations sur le canal Baidu pour une application.	Lecture	channel*		
GetCampaign	Accorde l'autorisation de récupérer des informations sur une campagne spécifique	Lecture	campaign*		
GetCampaignActivities	Accorde l'autorisation de récupérer des informations sur les activités effectuées par une campagne.	List	campaign*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCampaignDateRangeKpi	Accorde l'autorisation de récupérer (requêtes) des données pré-agrégées pour fournir une métrique standard qui s'applique à une campagne.	Lecture	campaign-metrics*		
GetCampaignVersion	Accorde l'autorisation de récupérer des informations sur la version d'une campagne spécifique	Lecture	campaign*		
GetCampaignVersions	Accorde l'autorisation de récupérer des informations sur les versions actuelles et antérieures d'une campagne.	List	campaign*		
GetCampaigns	Accorde l'autorisation de récupérer des informations sur toutes les campagnes pour une application.	List	app*		
GetChannels	Accorde l'autorisation d'obtenir toutes les informations sur les canaux pour votre application	List	channels*		
GetEmailChannel	Accorde l'autorisation d'obtenir des informations sur le canal d'e-mail dans une application.	Lecture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEmailTemplate	Accorde l'autorisation de récupérer des informations sur une version spécifique ou active d'un modèle d'e-mail.	Lecture	template*		
GetEndpoint	Accorde l'autorisation de récupérer des informations sur un point de terminaison spécifique	Lecture	endpoint*		
GetEventStream	Accorde l'autorisation de récupérer des informations sur le flux d'événements pour une application.	Lecture	event-stream*		
GetExportJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'exportation spécifique.	Lecture	export-job*		
GetExportJobs	Accorde l'autorisation de récupérer une liste de toutes les tâches d'exportation pour une application.	List	app*		
GetGcmChannel	Accorde l'autorisation de récupérer des informations sur le canal GCM pour une application.	Lecture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetImportJob	Accorde l'autorisation de récupérer des informations sur une tâche d'importation spécifique	Lecture	import-job*		
GetImportJobs	Accorde l'autorisation de récupérer des informations sur toutes les tâches d'importation pour une application.	List	app*		
GetInAppMessages	Accorde l'autorisation de récupérer les messages intégrés à l'application pour l'identifiant de point de terminaison donné	Lecture	app*		
GetInAppTemplate	Accorde l'autorisation de récupérer des informations sur une version spécifique ou active d'un modèle de message in-app	Lecture	template*		
GetJourney	Accorde l'autorisation de récupérer des informations sur un parcours spécifique	Lecture	journey*		
GetJourneyDateRangeKpi	Accorde l'autorisation de récupérer (requêtes) des données pré-agrégées pour fournir une métrique d'engagement standard qui s'applique à un parcours.	Lecture	journey-metrics*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetJourneyExecutionActivityMetrics	Accorde l'autorisation de récupérer (requêtes) des données pré-agrégées pour fournir une métrique d'exécution standard qui s'applique à une activité du parcours.	Lecture	journey-execution-activity-metrics*		
GetJourneyExecutionMetrics	Accorde l'autorisation de récupérer (requêtes) des données pré-agrégées pour fournir une métrique d'exécution standard qui s'applique à un parcours.	Lecture	journey-execution-metrics*		
GetJourneyRunExecutionActivityMetrics	Accorde l'autorisation de récupérer (requêtes) des données pré-agrégées pour fournir une métrique d'exécution standard qui s'applique à une activité du parcours.	Lecture	journey*		
GetJourneyRunExecutionMetrics	Accorde l'autorisation de récupérer (requêtes) des données pré-agrégées pour fournir une métrique d'exécution standard qui s'applique à un parcours.	Lecture	journey*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetJourneyRuns	Accorde l'autorisation de récupérer des informations sur tous les parcours pour une application.	List	journey*		
GetPushTemplate	Accorde l'autorisation de récupérer des informations sur une version spécifique ou active d'un modèle de notification push.	Lecture	template*		
GetRecommenderConfiguration	Accorde l'autorisation de récupérer des informations sur une configuration Amazon Pinpoint pour un modèle de recommandation.	Lecture	recommender*		
GetRecommenderConfigurations	Accorde l'autorisation de récupérer des informations sur toutes les configurations de modèle de recommandation associées à un compte Amazon Pinpoint.	List	recommenders*		
GetReports [autorisation uniquement]	Autorise le ciblage mobile : GetReports	Lecture	reports*		
GetSegment	Accorde l'autorisation de récupérer des informations sur un segment spécifique	Lecture	segment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSegmentExportJobs	Accorde l'autorisation de récupérer des informations sur les tâches qui exportent les définitions de point de terminaison à partir de segments vers Amazon S3.	List	segment*		
GetSegmentImportJobs	Accorde l'autorisation de récupérer des informations sur les tâches qui créent des segments en important les définitions de point de terminaison à partir de	List	segment*		
GetSegmentVersion	Accorde l'autorisation de récupérer des informations sur la version d'un segment spécifique	Lecture	segment*		
GetSegmentVersions	Accorde l'autorisation de récupérer des informations sur les versions actuelles et antérieures d'un segment.	List	segment*		
GetSegments	Accorde l'autorisation de récupérer des informations sur les segments pour une application.	List	app*		
GetSmsChannel	Accorde l'autorisation d'obtenir des informations sur le canal SMS d'une application.	Lecture	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSmsTemplate	Accorde l'autorisation de récupérer des informations sur une version spécifique ou active d'un modèle de message SMS.	Lecture	template*		
GetUserEndpoints	Accorde l'autorisation de récupérer des informations sur les points de terminaison qui sont associés à un ID d'utilisateur.	Lecture	user*		
GetVoiceChannel	Accorde l'autorisation d'obtenir des informations sur le canal vocal d'une application.	Lecture	channel*		
GetVoiceTemplate	Accorde l'autorisation de récupérer des informations sur une version spécifique ou active d'un modèle de message vocal.	Lecture	template*		
ListJourneys	Accorde l'autorisation de récupérer des informations sur tous les parcours pour une application.	List	app*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	app		
			campaign		
			journey		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			segment		
			template		
ListTemplateVersions	Accorde l'autorisation de récupérer toutes les versions d'un modèle spécifique.	List	template*		
ListTemplates	Accorde l'autorisation de récupérer les métadonnées relatives aux modèles interrogés.	List	templates*		
PhoneNumberValidate	Accorde l'autorisation d'obtenir les métadonnées pour un numéro de téléphone, par exemple le type de numéro (téléphone portable, fixe ou VoIP), l'emplacement et le fournisseur.	Lecture	phone-number-validate*		
PutEventStream	Accorde l'autorisation de créer ou de mettre à jour un flux d'événement pour une application.	Écrire	event-stream*		
PutEvents	Accorde l'autorisation de créer ou de mettre à jour des événements pour une application.	Écrire	events*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveAttributes	Accorde l'autorisation de supprimer les attributs pour une application.	Écrire	attribute*		
SendMessages	Accorde l'autorisation d'envoyer un message SMS ou une notification push à des points de terminaison spécifiques.	Écrire	messages*		
SendOTPMessage	Accorde l'autorisation d'envoyer un code OTP à un utilisateur de votre application	Écrire	otp*		
SendUsersMessages	Accorde l'autorisation d'envoyer un message SMS ou une notification push à tous les points de terminaison qui sont associés à un ID d'utilisateur spécifique.	Écrire	messages*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	app		
			campaign		
			journey		
			segment		
			template		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	app		
			campaign		
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateAdmChannel	Accorde l'autorisation de mettre à jour le canal Amazon Device Messaging (ADM) pour une application.	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApnsChannel	Accorde l'autorisation de mettre à jour le canal du service de notification push Apple (APNs) pour une application	Écrire	channel*		
UpdateApnsSandboxChannel	Accorde l'autorisation de mettre à jour le canal sandbox du service de notification push Apple (APNs) pour une application	Écrire	channel*		
UpdateApnsVoipChannel	Accorde l'autorisation de mettre à jour le canal VoIP du service de notification push Apple (APNs) pour une application	Écrire	channel*		
UpdateApnsVoipSandboxChannel	Accorde l'autorisation de mettre à jour le canal sandbox VoIP du service de notification push Apple (APNs) pour une application	Écrire	channel*		
UpdateApplicationSettings	Accorde l'autorisation de mettre à jour les paramètres par défaut pour une application.	Écrire	app*		
UpdateBaiduChannel	Accorde l'autorisation de mettre à jour le canal Baidu pour une application.	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCampaign	Accorde l'autorisation de mettre à jour une campagne spécifique	Écrire	campaign*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEmailChannel	Accorde l'autorisation de mettre à jour le canal de messagerie électronique pour une application.	Écrire	channel*		
UpdateEmailTemplate	Accorde l'autorisation de mettre à jour un modèle d'e-mail spécifique sous la même version ou de générer une nouvelle version.	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEndpoint	Accorde l'autorisation de créer un point de terminaison ou de mettre à jour les informations d'un point de terminaison	Écrire	endpoint*		
UpdateEndpointsBatch	Accorde l'autorisation de créer ou de mettre à jour les points de terminaison sous la forme d'une opération par lot.	Écrire	app*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGcmChannel	Accorde l'autorisation de mettre à jour la clé d'API Firebase Cloud Messaging (FCM) ou Google Cloud Messaging (GCM) qui permet d'envoyer des notifications push à votre application Android.	Écrire	channel*		
UpdateInAppTemplate	Accorde l'autorisation de mettre à jour un modèle de message in-app spécifique sous la même version ou de générer une nouvelle version	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourney	Accorde l'autorisation de mettre à jour un parcours spécifique	Écrire	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourneyState	Accorde l'autorisation de mettre à jour un état de parcours spécifique	Écrire	journey*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePushTemplate	Accorde l'autorisation de mettre à jour un modèle de notification push spécifique sous la même version ou de générer une nouvelle version.	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateRecommenderConfiguration	Accorde l'autorisation de mettre à jour une configuration Amazon Pinpoint pour un modèle de recommandation.	Écrire	recommender*		
UpdateSegment	Accorde l'autorisation de mettre à jour un segment spécifique	Écrire	segment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSmsChannel	Accorde l'autorisation de mettre à jour le canal SMS pour une application.	Écrire	channel*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSmsTemplate	Accorde l'autorisation de mettre à jour un modèle de message SMS spécifique sous la même version ou de générer une nouvelle version.	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTemplateActiveVersion	Accorde l'autorisation de mettre à jour le paramètre de version active d'un modèle spécifique.	Écrire	template*		
UpdateVoiceChannel	Accorde l'autorisation de mettre à jour le canal vocal pour une application.	Écrire	channel*		
UpdateVoiceTemplate	Accorde l'autorisation de mettre à jour un modèle de message vocal spécifique sous la même version ou de générer une nouvelle version.	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyOTPMessage	Permet de vérifier la validité des mots de passe à usage unique (OTPs)	Écrire	verify-otp*		

Types de ressources définis par Amazon Pinpoint

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
app	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey}
apps	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/*`	
campaign	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}`	aws:ResourceTag/${TagKey}
journey	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}`	aws:ResourceTag/${TagKey}
journeys	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys`	
segment	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/segments/${SegmentId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:mobiletargeting:${Region}:${Account}:templates/${TemplateName}/${TemplateType}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
templates	arn:${Partition}:mobiletargeting:${Region}:${Account}:templates	
recommender	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/${RecommenderId}	
recommenders	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/*	
phone-number-validate	arn:${Partition}:mobiletargeting:${Region}:${Account}:phone/number/validate	
channels	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels	
channel	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels/${ChannelType}	
event-stream	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/eventstream	
events	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/events	
messages	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/messages	

Types de ressources	ARN	Clés de condition
verify-otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/verify-otp	
otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/otp	
attribute	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/attributes/${AttributeType}	
user	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/users/${UserId}	
endpoint	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/endpoints/${EndpointId}	
import-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/import/${JobId}	
export-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/export/${JobId}	
application-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/kpis/daterange/${KpiName}	
campaign-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}/kpis/daterange/${KpiName}	

Types de ressources	ARN	Clés de condition
journey-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/kpis/daterange/${KpiName}	
journey-execution-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/execution-metrics	
journey-execution-activity-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/activities/${JourneyActivityId}/execution-metrics	
reports	arn:${Partition}:mobiletargeting:${Region}:${Account}:reports	

Clés de condition pour Amazon Pinpoint

Amazon Pinpoint définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'une clé qui est présente dans la demande envoyée par l'utilisateur au service pinpoint.	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction d'une paire de clé et de valeur de balise	String
aws:TagKeys	Filtre l'accès en fonction de la liste de tous les noms de clé de balise présents dans la demande envoyée par l'utilisateur au service pinpoint.	ArrayOfString

Actions, ressources et clés de condition pour Amazon Pinpoint Email Service

Amazon Pinpoint Email Service (préfixe de service : `ses`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Pinpoint Email Service
- Types de ressources définis par Amazon Pinpoint Email Service
- Clés de condition pour Amazon Pinpoint Email Service

Actions définies par Amazon Pinpoint Email Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfigurationSet	Accorde l'autorisation de créer un ensemble de configuration	Écriture		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Accorde l'autorisation de créer une destination d'événement d'ensemble de configurations	Écriture	configuration-set* ses:ApiVersion aws:ResourceTag/${TagKey}		
CreateDedicatedIpPool	Accorde l'autorisation de créer un nouveau groupe d'adresses IP dédiées	Écriture		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Accorde l'autorisation de créer un test prédictif de placement dans la boîte de réception	Écriture	identity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Accorde l'autorisation de démarrer un processus de vérification d'une identité d'adresse e-mail	Écriture		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Accorde l'autorisation de supprimer un ensemble de configurations existant	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConfigurationSetEventDestination	Accorde l'autorisation de supprimer une destination d'événement	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Accorde l'autorisation de supprimer un groupe d'adresses IP dédié	Écriture	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Accorde l'autorisation de supprimer une identité d'adresse e-mail que vous avez précédemment vérifiée	Écriture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Accorde l'autorisation d'obtenir des informations sur le statut et les fonctionnalités de l'envoi d'e-mail	Lecture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBlacklistReports	Accorde l'autorisation de récupérer une liste des listes de refus sur lesquelles vos adresses IP dédiées apparaissent	Lecture		ses:ApiVersion	
GetConfigurationSet	Accorde l'autorisation d'obtenir des informations sur un ensemble de configurations existant	Lecture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Accorde l'autorisation de récupérer une liste des destinations d'événement qui sont associées à un ensemble de configurations	Lecture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	Accorde l'autorisation d'obtenir des informations sur une adresse IP dédiée	Lecture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDedicatedIps	Accorde l'autorisation de répertorier des adresses IP dédiées qui sont associées à votre compte	Lecture	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDeliverabilityDashboardOptions	Accorde l'autorisation d'obtenir le statut du tableau de bord de délivrabilité	Lecture		ses:ApiVersion	
GetDeliverabilityTestReport	Accorde l'autorisation de récupérer les résultats d'un test prédictif de placement dans la boîte de réception	Lecture	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Accorde l'autorisation de récupérer toutes les données de délivrabilité pour une campagne spécifique	Lecture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDomainStatisticsReport	Accorde l'autorisation de récupérer des taux d'engagement et de placement de la boîte de réception pour les domaines que vous utilisez pour envoyer des e-mails	Lecture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Accorde l'autorisation d'obtenir des informations sur une identité spécifique associée à votre compte	Lecture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Accorde l'autorisation de répertorier tous les ensembles de configuration associés à votre compte	Liste		ses:ApiVersion	
ListDedicatedIpPools	Accorde l'autorisation de répertorier tous les groupes d'adresses IP dédiées qui existent dans votre compte	Liste		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDeliverabilityTestReports	Accorde l'autorisation de récupérer une liste des tests prédictifs de placement dans la boîte de réception que vous avez effectués, quel que soit leur statut	Liste		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Accorde l'autorisation de récupérer des données de délivrabilité pour toutes les campagnes ayant utilisé un domaine spécifique pour envoyer des e-mails pendant une période spécifiée	Lecture		ses:ApiVersion	
ListEmailIdentities	Accorde l'autorisation de répertorier toutes les identités d'e-mail associées à votre compte	Liste		ses:ApiVersion	
ListTagsForResource	Accorde l'autorisation de récupérer une liste des balises (clés et valeurs) qui sont associées à une ressource spécifique	Lecture	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion	
PutAccountDedicatedIpWarmupAttributes	Accorde l'autorisation d'activer ou de désactiver la fonction de préparation automatique pour les adresses IP dédiées	Écriture		ses:ApiVersion	
PutAccountSendingAttributes	Accorde l'autorisation d'activer ou de désactiver la possibilité de votre compte d'envoyer des e-mails	Écriture		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Accorde l'autorisation d'association un ensemble de configurations à un groupe d'adresses IP dédiées	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Accorde l'autorisation d'activer ou de désactiver la collecte des métriques de réputation pour les e-mails que vous envoyez à l'aide d'un ensemble de configurations	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutConfigurationSetSendingOptions	Accorde l'autorisation d'activer ou de désactiver l'envoi des messages qui utilisent un ensemble de configurations spécifique	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Accorde l'autorisation de spécifier un nom de domaine personnalisé à utiliser pour les éléments de suivi des ouvertures et des clics dans les e-mails que vous envoyez à l'aide d'un ensemble de configurations spécifique	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Accorde l'autorisation de déplacer une adresse IP dédiée vers un groupe d'adresses IP dédiées existant	Écriture	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Accorde l'autorisation d'activer des attributs de mise en route IP dédiés	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDeliverabilityDashboardOption	Accorde l'autorisation d'activer ou de désactiver le tableau de bord de délivrabilité	Écriture		ses:ApiVersion	
PutEmailIdentityDkimAttributes	Accorde l'autorisation d'activer ou de désactiver l'authentification DKIM pour une identité d'e-mail	Écriture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Accorde l'autorisation d'activer ou de désactiver le transfert de commentaires pour une identité	Écriture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Accorde l'autorisation d'activer ou de désactiver la configuration de domaine Mail-From personnalisée pour une identité d'e-mail	Écriture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
SendEmail	Accorde l'autorisation d'envoyer un e-mail	Écriture	identity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises (clés et valeurs) à la ressource spécifiée	Balisage	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises (clés et valeurs) de la ressource spécifiée	Balisage	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConfigurationSetEventDestination	Accorde l'autorisation de mettre à jour la configuration d'une destination d'événement pour un ensemble de configurations	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon Pinpoint Email Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Pinpoint Email Service

Le service de messagerie Amazon Pinpoint définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString
ses:ApiVersion	Filtre les actions en fonction de la version de l'API SES	String
ses:FeedbackAddress	Filtre les actions en fonction de l'adresse « Return-Path », qui spécifie l'adresse à laquelle les retours à l'expéditeur et les réclamations sont envoyés via le transfert de commentaires par e-mail	Chaîne

Clés de condition	Description	Type
ses:FromAddress	Filtre les actions en fonction de l'adresse « From » d'un message	Chaîne
ses:FromDisplayName	Filtre les actions en fonction de l'adresse « From » utilisée comme nom d'affichage d'un message	Chaîne
ses:Recipients	Filtre les actions en fonction des adresses des destinataires d'un message, qui incluent les adresses « To », « CC » et « BCC »	ArrayOfString

Actions, ressources et clés de condition pour Amazon Pinpoint SMS and Voice Service

Amazon Pinpoint SMS and Voice Service (préfixe de service : `sms-voice`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Pinpoint SMS and Voice Service
- Types de ressources définis par Amazon Pinpoint SMS and Voice Service
- Clés de condition pour Amazon Pinpoint SMS and Voice Service

Actions définies par Amazon Pinpoint SMS and Voice Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfigurationSet	Crée un ensemble de configurations. Une fois que vous avez créé l'ensemble de configurations, vous pouvez ajouter une ou plusieurs destinations d'événement.	Écriture			
CreateConfigurationSetEventDestination	Crée un événement de destination dans un ensemble de configurations.	Écriture			iam:PassRole
DeleteConfigurationSet	Supprime un ensemble de configurations existant.	Écriture			
DeleteConfigurationSetEventDestination	Supprime un événement de destination dans un ensemble de configurations.	Écriture			
GetConfigurationSetEventDestinations	Obtient des informations sur une destination d'événement, y compris les types d'événements signalés, l'ARN (Amazon Resource Name) de la destination et le nom de la destination de l'événement.	Lecture			
ListConfigurationSets	Renvoie une liste d'ensembles de configurations. Cette opération rapporte seulement les ensembles de configura	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	tions qui sont associés à votre compte dans la Région AWS actuelle.				
SendVoiceMessage	Crée un nouveau message vocal et l'envoie au numéro de téléphone du destinataire.	Écriture			
UpdateConfigurationSetEventDestination	Met à jour une destination d'événement dans un ensemble de configurations. Une destination d'événement est un emplacement pour vos appels vocaux au sujet desquels vous publiez des informations. Par exemple, vous pouvez enregistrer un événement sur une CloudWatch destination Amazon en cas d'échec d'un appel.	Écrire			iam:PassRole

Types de ressources définis par Amazon Pinpoint SMS and Voice Service

Amazon Pinpoint SMS et Voice Service ne prennent pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à Amazon Pinpoint SMS et Voice Service, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Amazon Pinpoint SMS and Voice Service

Pinpoint SMS Voice ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte

globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Polly

Amazon Polly (préfixe de service : `polly`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Polly
- Types de ressources définis par Amazon Polly
- Clés de condition pour Amazon Polly

Actions définies par Amazon Polly

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut

un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLexicon	Accorde l'autorisation de supprimer le lexique de	Écrire	lexicon*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	prononciation spécifié stocké dans un Région AWS				
DescribeVoices	Octroie l'autorisation de décrire la liste des voix qui peuvent être utilisées lors de la demande de synthèse vocale	List			
GetLexicon	Accorde l'autorisation de récupérer le contenu du lexique de prononciation spécifié stocké dans un Région AWS	Lecture	lexicon*		
GetSpeechSynthesisTask	Octroie l'autorisation d'obtenir des informations sur une tâche spécifique de synthèse vocale	Lecture			
ListLexicons	Permet de répertorier les lexiques de prononciation stockés dans un Région AWS	List			
ListSpeechSynthesisTasks	Octroie l'autorisation de répertorier les tâches de synthèse vocale demandées	List			
PutLexicon	Autorise le stockage d'un lexique de prononciation dans un Région AWS	Écrire	lexicon*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartSpeechSynthesisStream	Donne l'autorisation d'effectuer une synthèse avec un streaming bidirectionnel	Lecture	lexicon		
StartSpeechSynthesisTask	Octroie l'autorisation de synthétiser des entrées longues à l'emplacement S3 fourni	Écrire	lexicon		s3:PutObject
SynthesizeSpeech	Octroie l'autorisation d'effectuer la synthèse vocale	Lecture	lexicon		

Types de ressources définis par Amazon Polly

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
lexicon	`arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}`	

Clés de condition pour Amazon Polly

Polly ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour la liste de AWS prix

AWS La liste de prix (préfixe de service :`pricing`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Price List
- Types de ressources définis par la liste de AWS prix
- Clés de condition pour la liste de AWS prix

Actions définies par AWS Price List

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeServices	Accorde l'autorisation de récupérer une description détaillée de tous les services (paginés) (si serviceCode n'est pas défini) ou d'un service particulier (si serviceCode est donné).	Lecture			
GetAttributeValues	Accorde l'autorisation de récupérer toutes les valeurs possibles (paginées) pour un attribut donné	Lecture			
GetPriceListFileUrl	Octroie l'autorisation de récupérer l'URL du fichier de liste des prix pour les paramètres donnés	Lecture			
GetProducts	Accorde l'autorisation de récupérer tous les produits correspondant aux critères de recherche donnés	Lecture			
ListPriceLists	Octroie l'autorisation de répertorier toutes les listes de prix éligibles (paginées) pour les paramètres donnés	Lecture			

Types de ressources définis par la liste de AWS prix

AWS La liste de prix ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Price List, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour la liste de AWS prix

Price List ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le AWS PricingPlanManager service

AWS PricingPlanManager Le service (préfixe de service :`pricingplanmanager`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS PricingPlanManager service
- Types de ressources définis par le AWS PricingPlanManager service
- Clés de condition pour le AWS PricingPlanManager service

Actions définies par le AWS PricingPlanManager service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateResourcesToSubscription	Accorde l'autorisation d'associer des ressources à un abonnement	Écrire			
CancelSubscription	Autorise l'annulation d'un abonnement	Écrire			
CancelSubscriptionChange	Autorise l'annulation d'une modification en attente d'un abonnement	Écrire			
CreateSubscription	Accorde l'autorisation de créer un abonnement	Écrire			
DisassociateResourcesFromSubscription	Accorde l'autorisation de dissocier les ressources d'un abonnement	Écrire			
GetSubscription	Accorde l'autorisation d'obtenir les détails d'un abonnement	Lecture			
ListSubscriptions	Accorde l'autorisation de répertorier les abonnements dans votre compte	Lecture			
UpdateSubscription	Autorise la mise à jour d'un abonnement	Écrire			

Types de ressources définis par le AWS PricingPlanManager service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
subscription	`arn:${Partition}:pricingplanmanager::${Account}:subscription/${SubscriptionId}`	

Clés de condition pour le AWS PricingPlanManager service

PricingPlanManager ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Private CA Connector for Active Directory

AWS Le connecteur CA privé pour Active Directory (préfixe de service :`pca-connector-ad`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Private CA Connector pour Active Directory
- Types de ressources définis par AWS Private CA Connector pour Active Directory
- Clés de condition pour AWS Private CA Connector pour Active Directory

Actions définies par AWS Private CA Connector pour Active Directory

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConnector	Accorde l'autorisation de créer un connecteur dans votre compte	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:GetCertificateAuthorityCertificate acm-pca:I

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ssueCertificate ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
CreateDirectoryRegistration	Accorde l'autorisation d'en créer un DirectoryRegistration dans votre compte	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:DescribeDirectories
CreateServicePrincipalName	Accorde l'autorisation de créer un ServicePrincipalName pour DirectoryRegistration	Écrire	DirectoryRegistration*		ds:UpdateAuthorizedApplication
CreateTemplate	Accorde l'autorisation de créer un modèle pour un connecteur	Écrire	Connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTemplateGroupAccessControlEntry	Accorde l'autorisation de créer un TemplateGroupAccessControlEntry pour un modèle	Écrire	Template*		
DeleteConnector	Accorde l'autorisation de supprimer un connecteur dans votre compte	Écrire	Connector*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteDirectoryRegistration	Accorde l'autorisation de supprimer un Directory Registration élément de votre compte	Écrire	Directory Registration*		ds:UnauthorizeApplication ds:UpdateAuthorizedApplication

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteServicePrincipalName	Accorde l'autorisation de supprimer un ServicePrincipalName pour un Directory Registration	Écrire	Directory Registration*		ds:UpdateAuthorizedApplication
DeleteTemplate	Accorde l'autorisation de supprimer un modèle pour un connecteur	Écrire	Template*		
DeleteTemplateGroupAccessControlEntry	Accorde l'autorisation de supprimer un TemplateGroupAccessControlEntry pour un modèle	Écrire	Template*		
GetConnector	Accorde l'autorisation d'obtenir un connecteur dans votre compte	Lecture	Connector*		
GetDirectoryRegistration	Accorde l'autorisation d'accéder DirectoryRegistration à votre compte	Lecture	Directory Registration*		
GetServicePrincipalName	Donne l'autorisation d'obtenir un ServicePrincipalName pour DirectoryRegistration	Lecture	Directory Registration*		
GetTemplate	Accorde l'autorisation d'obtenir un modèle pour un connecteur	Lecture	Template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTemplateGroupAccessControlEntry	Accorde l'autorisation d'TemplateGroupAccessControlEntry obtenir un modèle	Lecture	Template*		
ListConnectors	Accorde l'autorisation de répertorier les connecteurs de votre compte	List			
ListDirectoryRegistrations	Accorde l'autorisation de les répertorier DirectoryRegistrations dans votre compte	List			
ListServicePrincipalNames	Accorde l'autorisation de mettre en vente le ServicePrincipalNames pour un DirectoryRegistration	List	DirectoryRegistration*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une pca-connector-ad ressource dans votre compte	Lecture			
ListTemplateGroupAccessControlEntries	Accorde l'autorisation de répertorier le TemplateGroupAccessControlEntries pour un modèle	List	Template*		
ListTemplates	Accorde l'autorisation de répertorier les modèles pour un connecteur	List	Connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'étiqueter une pca-connector-ad ressource dans votre compte	Identification	Connector		
			Directory Registration		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer le tag d'une pca-connector-ad ressource dans votre compte	Identification	Connector		
			Directory Registration		
			Template		
				aws:TagKeys	
UpdateTemplate	Accorde l'autorisation de mettre à jour un modèle pour un connecteur	Écrire	Template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTemplateGroupAccessControlEntry	Accorde l'autorisation de mettre à jour un TemplateGroupAccessControlEntry pour un modèle	Écrire	Template*		

Types de ressources définis par AWS Private CA Connector pour Active Directory

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Connector	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}
Directory Registration	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:directory-registration/${DirectoryId}`	aws:ResourceTag/${TagKey}
Template	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}/template/${TemplateId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Private CA Connector pour Active Directory

AWS Le connecteur CA privé pour Active Directory définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balises transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Private CA Connector for SCEP

AWS Le connecteur CA privé pour SCEP (préfixe de service :`pca-connector-scep`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Private CA Connector pour SCEP

- Types de ressources définis par AWS Private CA Connector pour SCEP
- Clés de condition pour le connecteur CA AWS privé pour SCEP

Actions définies par AWS Private CA Connector pour SCEP

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateChallenge	Accorde l'autorisation de créer un défi pour un connecteur	Écrire	Connector *		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Autorise la création d'un connecteur SCEP dans votre compte	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					acm-pca:GetCertificateAuthorityCertificate acm-pca:IssueCertificate
DeleteChallenge	Accorde l'autorisation de supprimer un défi pour un connecteur	Écrire	Challenge*		
DeleteConnector	Autorise la suppression d'un connecteur SCEP dans votre compte	Écrire	Connector*		
GetChallengeMetadata	Accorde l'autorisation de relever un défi pour un connecteur	Lecture	Challenge*		
GetChallengePassword	Accorde l'autorisation d'obtenir un mot de passe de défi pour un connecteur	Lecture	Challenge*		
GetConnector	Autorise l'accès à un connecteur SCEP sur votre compte	Lecture	Connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListChallengeMetadata	Accorde l'autorisation de répertorier les défis pour un connecteur	List			
ListConnectors	Accorde l'autorisation de répertorier les connecteurs SCEP dans votre compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une pca-connector-scep ressource dans votre compte	Lecture			
TagResource	Accorde l'autorisation d'étiqueter une pca-connector-scep ressource dans votre compte	Identification	Challenge		
			Connector		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer le tag d'une pca-connector-scep ressource dans votre compte	Identification	Challenge		
			Connector		
				aws:TagKeys	

Types de ressources définis par AWS Private CA Connector pour SCEP

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Challenge	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}/challenge/${ChallengeId}`	aws:ResourceTag/${TagKey}
Connector	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}

Clés de condition pour le connecteur CA AWS privé pour SCEP

AWS Le connecteur CA privé pour SCEP définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour l'autorité de certification AWS privée

AWS L'autorité de certification privée (préfixe de service :`acm-pca`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'autorité de certification AWS privée
- Types de ressources définis par l'autorité de certification AWS privée
- Clés de condition pour l'autorité de certification AWS privée

Actions définies par l'autorité de certification AWS privée

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCertificateAuthority	Accorde l'autorisation de créer une autorité de certification AWS privée ainsi que la clé privée et la configuration associées	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCertificateAuthorityAuditReport	Accorde l'autorisation de créer un rapport d'audit pour une autorité de certification AWS privée	Écrire	certificate-authority*		
CreatePermission	Accorde l'autorisation de créer une autorisation pour une autorité de certification AWS privée	Gestion des autorisations	certificate-authority*		
DeleteCertificateAuthority	Accorde l'autorisation de supprimer une autorité de certification AWS privée ainsi que la clé privée et la configuration associées	Écrire	certificate-authority*		
DeletePermission	Accorde l'autorisation de supprimer une autorisation pour une autorité de certification AWS privée	Gestion des autorisations	certificate-authority*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePolicy	Accorde l'autorisation de supprimer la politique d'une autorité de certification AWS privée	Gestion des autorisations	certificate-authority*		
DescribeCertificateAuthority	Accorde l'autorisation de renvoyer une liste des champs de configuration et d'état contenus dans l'autorité de certification AWS privée spécifiée	Lecture	certificate-authority*		
DescribeCertificateAuthorityAuditReport	Accorde l'autorisation de renvoyer le statut et les informations relatives à un rapport d'audit de AWS Private CA	Lecture	certificate-authority*		
GetCertificate	Accorde l'autorisation de récupérer un certificat CA AWS privé et une chaîne de certificats pour l'autorité de certification spécifiée par un ARN	Lecture	certificate-authority*		
GetCertificateAuthorityCertificate	Accorde l'autorisation de récupérer un certificat CA AWS privé et une chaîne de certificats pour l'autorité de certification spécifiée par un ARN	Lecture	certificate-authority*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCertificateAuthorityCsr	Accorde l'autorisation de récupérer une demande de signature de certificat CA AWS privée (CSR) pour l'autorité de certification spécifiée par un ARN	Lecture	certificate-authority*		
GetPolicy	Accorde l'autorisation de récupérer la politique sur une autorité de certification AWS privée	Lecture	certificate-authority*		
ImportCertificateAuthorityCertificate	Accorde l'autorisation d'importer un SSL/TLS certificat dans une autorité de certification AWS privée afin de l'utiliser comme certificat d'autorité de certification AWS privée	Écrire	certificate-authority*		
IssueCertificate	Autorise l'émission d'un certificat CA AWS privé	Écrire	certificate-authority*		
				acm-pca:TemplateArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCertificateAuthorities	Accorde l'autorisation de récupérer une liste de l'autorité de certification de l'autorité ARNs de certification AWS privée et un résumé du statut de chaque autorité de certification dans le compte appelant	List			
ListPermissions	Accorde l'autorisation de répertorier les autorisations qui ont été appliquées à l'autorité de certification AWS privée CA	Lecture	certificate-authority*		
ListTags	Accorde l'autorisation de répertorier les balises qui ont été appliquées à l'autorité de certification AWS Private CA	Lecture	certificate-authority*		
PutPolicy	Accorde l'autorisation d'appliquer une politique à une autorité de certification AWS privée	Gestion des autorisations	certificate-authority*		
RestoreCertificateAuthority	Accorde l'autorisation de restaurer une autorité de certification AWS privée de l'état supprimé à l'état dans lequel elle se trouvait au moment de sa suppression	Écrire	certificate-authority*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RevokeCertificate	Accorde l'autorisation de révoquer un certificat émis par une autorité de certification AWS privée	Écrire	certificate-authority*		
TagCertificateAuthority	Accorde l'autorisation d'ajouter une ou plusieurs balises à une autorité de certification AWS privée	Identification	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCertificateAuthority	Accorde l'autorisation de supprimer une ou plusieurs balises d'une autorité de certification AWS privée	Identification	certificate-authority*	aws:RequestTag/${TagKey}	
				aws:TagKeys	
UpdateCertificateAuthority	Accorde l'autorisation de mettre à jour la configuration d'une autorité de certification AWS privée	Écrire	certificate-authority*		

Types de ressources définis par l'autorité de certification AWS privée

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey}

Clés de condition pour l'autorité de certification AWS privée

AWS L'autorité de certification privée définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
acm-pca:TemplateArn	Filtre l'accès en fonction de l'ARN du modèle de certificat utilisé dans la demande d'émission de certificat.	ARN
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS PrivateLink

AWS PrivateLink (préfixe de service :`vpce`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS PrivateLink
- Types de ressources définis par AWS PrivateLink
- Clés de condition pour AWS PrivateLink

Actions définies par AWS PrivateLink

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowMultiRegion [autorisation uniquement]	Accorde l'autorisation de gérer les points de terminaison VPC multirégionaux et les configurations des services de point de terminaison VPC	Écrire	vpc-endpoint		
			vpc-endpoint-service		

Types de ressources définis par AWS PrivateLink

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
vpc-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint/${VpcEndpointId}`	
vpc-endpoint-service	`arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service/${VpcEndpointServiceId}`	

Clés de condition pour AWS PrivateLink

VPC Endpoints ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément des déclarations de `Condition` politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Proton

AWS Proton (préfixe de service :`proton`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Proton
- Types de ressources définis par AWS Proton
- Clés de condition pour AWS Proton

Actions définies par AWS Proton

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptEnvironmentAccountConnection	Accorde l'autorisation de refuser la connexion à un compte d'environnement à partir d'un autre compte d'environnement	Écrire	environment-account-connection*		
CancelComponentDeployment	Accorde l'autorisation d'annuler un déploiement de composants	Écrire	component*		
CancelEnvironmentDeployment	Accorde l'autorisation d'annuler un déploiement d'environnement	Écriture	environment*		
				proton:EnvironmentTemplate	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelServiceInstanceDeployment	Accorde l'autorisation d'annuler un déploiement d'instance de service	Écriture	service-instance*		
				proton:ServiceTemplate	
CancelServicePipelineDeployment	Accorde l'autorisation d'annuler un déploiement de pipeline de service	Écrire	service*		
				proton:ServiceTemplate	
CreateComponent	Accorde l'autorisation de créer un composant	Écrire	component*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironment	Accorde l'autorisation de créer un environnement	Écriture	environment*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} proton:EnvironmentTemplate	
CreateEnvironmentAccountConnection	Accorde l'autorisation de créer une connexion à un compte d'environnement	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplate	Accorde l'autorisation de créer un modèle d'environnement	Écrire	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEnvironmentTemplateMajorVersion	Accorde l'autorisation de créer une version majeure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place CreateEnvironmentTemplateVersion	Écrire	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMinorVersion	Accorde l'autorisation de créer une version mineure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place CreateEnvironmentTemplateVersion	Écrire	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateVersion	Accorde l'autorisation de créer une version d'un modèle d'environnement	Écrire	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRepository	Accorde l'autorisation de créer un référentiel	Écrire	repository*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Accorde l'autorisation de créer un service	Écrire	service*		codestar-connections:PassConnection
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceInstance	Accorde l'autorisation de créer une instance de service	Écrire	service-instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceSyncConfig	Accorde l'autorisation de créer une configuration de synchronisation de service	Écrire			
CreateServiceTemplate	Accorde l'autorisation de créer un modèle de service	Écrire	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateServiceTemplateMajorVersion	Accorde l'autorisation de créer une version majeure d'un modèle de service. OBSOLÈTE - à utiliser à la place CreateServiceTemplateVersion	Écrire	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMinorVersion	Accorde l'autorisation de créer une version mineure d'un modèle de service. OBSOLÈTE - à utiliser à la place CreateServiceTemplateVersion	Écrire	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateVersion	Accorde l'autorisation de créer une version d'un modèle de service	Écrire	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTemplateSyncConfig	Accorde l'autorisation de créer une config de synchronisation de modèle	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccountRoles	Accorde l'autorisation de supprimer les rôles de compte. OBSOLÈTE - à utiliser à la place UpdateAccountSettings	Écrire			
DeleteComponent	Accorde l'autorisation de supprimer un composant	Écrire	component*		
DeleteDeployment	Octroie l'autorisation de supprimer un déploiement.	Écrire	deployment*		
DeleteEnvironment	Accorde l'autorisation de supprimer un environnement	Écriture	environment*		
				proton:EnvironmentTemplate	
DeleteEnvironmentAccountConnection	Accorde l'autorisation de supprimer une connexion à un compte d'environnement	Écriture	environment-account-connection*		
DeleteEnvironmentTemplate	Accorde l'autorisation de supprimer un modèle d'environnement	Écrire	environment-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEnvironmentTemplateMajorVersion	Accorde l'autorisation de supprimer une version majeure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place DeleteEnvironmentTemplateVersion	Écrire	environment-template*		
DeleteEnvironmentTemplateMinorVersion	Accorde l'autorisation de supprimer une version mineure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place DeleteEnvironmentTemplateVersion	Écrire	environment-template*		
DeleteEnvironmentTemplateVersion	Accorde l'autorisation de supprimer une version d'un modèle d'environnement	Écrire	environment-template*		
DeleteRepository	Accorde l'autorisation de supprimer un référentiel	Écrire	repository*		
DeleteService	Accorde l'autorisation de supprimer un service	Écrire	service*		
				proton:ServiceTemplate	
DeleteServiceSyncConfig	Accorde l'autorisation de supprimer une configuration de synchronisation de service	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteServiceTemplate	Accorde l'autorisation de supprimer un modèle de service	Écrire	service-template*		
DeleteServiceTemplateMajorVersion	Accorde l'autorisation de supprimer une version majeure d'un modèle de service. OBSOLÈTE - à utiliser à la place DeleteServiceTemplateVersion	Écrire	service-template*		
DeleteServiceTemplateMinorVersion	Accorde l'autorisation de supprimer une version mineure d'un modèle de service. OBSOLÈTE - à utiliser à la place DeleteServiceTemplateVersion	Écrire	service-template*		
DeleteServiceTemplateVersion	Accorde l'autorisation de supprimer une version d'un modèle de service	Écrire	service-template*		
DeleteTemplateSyncConfig	Accorde l'autorisation de supprimer un TemplateSyncConfig	Écrire			
GetAccountRoles	Accorde l'autorisation d'obtenir les rôles de compte. OBSOLÈTE - à utiliser à la place GetAccountSettings	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountSettings	Accorde l'autorisation de décrire les paramètres d'un compte	Lecture			
GetComponent	Accorde l'autorisation de décrire un composant	Lecture	component*		
GetDeployment	Octroie l'autorisation de décrire un déploiement.	Lecture	deployment*		
GetEnvironment	Accorde l'autorisation de décrire un environnement	Read	environment*		
GetEnvironmentAccountConnection	Accorde l'autorisation de décrire une connexion à un compte d'environnement	Read	environment-account-connection*		
GetEnvironmentTemplate	Accorde l'autorisation de décrire un modèle d'environnement	Lecture	environment-template*		
GetEnvironmentTemplateMajorVersion	Accorde l'autorisation d'obtenir une version majeure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place GetEnvironmentTemplateVersion	Lecture	environment-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEnvironmentTemplateMinorVersion	Accorde l'autorisation d'obtenir une version mineure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place GetEnvironmentTemplateVersion	Lecture	environment-template*		
GetEnvironmentTemplateVersion	Accorde l'autorisation de décrire une version d'un modèle d'environnement	Lecture	environment-template*		
GetRepository	Accorde l'autorisation de décrire un référentiel	Lecture	repository*		
GetRepositorySyncStatus	Accorde l'autorisation d'obtenir le dernier statut de synchronisation d'un référentiel	Lecture			
GetResourceTemplateVersionStatusCounts	Accorde l'autorisation de répertorier les comptes de statut de la version du modèle de ressource	Lecture			
GetResourcesSummary	Accorde l'autorisation d'obtenir un récapitulatif des ressources	Lecture			
GetService	Accorde l'autorisation de décrire un service	Lecture	service*		
GetServiceInstance	Accorde l'autorisation de décrire une instance de service	Lecture	service-instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceInstanceSyncStatus	Accorde l'autorisation de décrire le statut de synchronisation d'une instance de service	Lecture			
GetServiceSyncBlockerSummary	Accorde l'autorisation de décrire les bloqueurs de synchronisation de service sur un service ou une instance de service	Lecture			
GetServiceSyncConfig	Accorde l'autorisation de décrire une configuration de synchronisation de service	Lecture			
GetServiceTemplate	Accorde l'autorisation de décrire un modèle de service	Lecture	service-template*		
GetServiceTemplateMajorVersion	Accorde l'autorisation d'obtenir une version majeure d'un modèle de service. OBSOLÈTE - à utiliser à la place GetServiceTemplateVersion	Lecture	service-template*		
GetServiceTemplateMinorVersion	Accorde l'autorisation d'obtenir une version mineure d'un modèle de service. OBSOLÈTE - à utiliser à la place GetServiceTemplateVersion	Lecture	service-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceTemplateVersion	Accorde l'autorisation de décrire une version d'un modèle de service	Lecture	service-template*		
GetTemplateSyncConfig	Accorde l'autorisation de décrire un TemplateSyncConfig	Lecture			
GetTemplateSyncStatus	Accorde l'autorisation de décrire le statut de synchronisation d'un modèle	Lecture			
ListComponentOutputs	Accorde l'autorisation de répertorier les sorties de composant	List	component*		
			deployment		
ListComponentProvisionedResources	Accorde l'autorisation de répertorier les ressources provisionnées de composant	List	component*		
ListComponents	Accorde l'autorisation de répertorier les composants	List	environment		
			service		
			service-instance		
ListDeployments	Accorde l'autorisation de répertorier les déploiements	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEnvironmentAccountConnections	Accorde l'autorisation de répertorier les connexions de compte d'environnement	List			
ListEnvironmentOutputs	Accorde l'autorisation de répertorier les sorties d'environnement	List	environment*		
			deployment		
ListEnvironmentProvisionedResources	Accorde l'autorisation de répertorier les ressources provisionnées d'environnement	List	environment*		
ListEnvironmentTemplateMajorVersions	Accorde l'autorisation de répertorier les versions majeures du modèle d'environnement. OBSOLÈTE - à utiliser à la place ListEnvironmentTemplateVersions	List	environment-template*		
ListEnvironmentTemplateMinorVersions	Accorde l'autorisation de répertorier les versions mineures d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place ListEnvironmentTemplateVersions	List	environment-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEnvironmentTemplateVersions	Accorde l'autorisation de répertorier les versions du modèle d'environnement	Liste	environment-template*		
ListEnvironmentTemplates	Accorde l'autorisation de répertorier les modèles d'environnement	Liste			
ListEnvironments	Accorde l'autorisation de répertorier les environnements	List			
ListRepositories	Accorde l'autorisation de répertorier les référentiels	List			
ListRepositorySyncDefinitions	Accorde l'autorisation de répertorier les définitions de synchronisation de référentiel	List			
ListServiceInstanceOutputs	Accorde l'autorisation de répertorier les sorties d'instance de service	List	service*		
			service-instance*		
			deployment		
ListServiceInstanceProvisionedResources	Accorde l'autorisation de répertorier les ressources provisionnées d'instance de service.	List	service*		
			service-instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceInstances	Accorde l'autorisation de répertorier les instances de service	List			
ListServiceInstanceOutputs	Accorde l'autorisation de répertorier les sorties de pipeline de service	List	service* deployment		
ListServicePipelineProvisionedResources	Accorde l'autorisation de répertorier les ressources provisionnées de pipeline de service	List	service*		
ListServiceTemplateMajorVersions	Accorde l'autorisation de répertorier les versions majeures d'un modèle de service. OBSOLÈTE - à utiliser à la place ListServiceTemplateVersions	List	service-template*		
ListServiceTemplateMinorVersions	Accorde l'autorisation de répertorier les versions mineures d'un modèle de service. OBSOLÈTE - à utiliser à la place ListServiceTemplateVersions	List	service-template*		
ListServiceTemplateVersions	Accorde l'autorisation de répertorier les versions d'un modèle de service	Liste	service-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceTemplates	Accorde l'autorisation de répertorier les modèles de service	Liste			
ListServices	Accorde l'autorisation de répertorier les services	List			
ListTagsForResource	Accorde l'autorisation de répertorier les étiquettes d'une ressource	Lecture	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
NotifyResourceDeploymentStatusChange	Accorde l'autorisation de notifier à Proton les changements de statut du déploiement des ressources	Écrire	environment		
			service-instance		
RejectEnvironmentAccountConnection	Accorde l'autorisation de refuser la connexion à un compte d'environnement à partir d'un autre compte d'environnement	Écrire	environment-account-connection*		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Balisage	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			service-template-version		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	component		
			environment		
			environment-account-connection		
			environment-template		
			environment-template-major-version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			service-template-version		
				aws:TagKeys	
UpdateAccountRoles	Accorde l'autorisation de mettre à jour les rôles de compte. OBSOLÈTE - à utiliser à la place UpdateAccountSettings	Écrire			iam:PassRole
UpdateAccountSettings	Accorde l'autorisation de mettre à jour les paramètres d'un compte	Écrire			iam:PassRole
UpdateComponent	Accorde l'autorisation de mettre à jour un composant	Écrire	component*		
UpdateEnvironment	Accorde l'autorisation de mettre à jour un environnement	Écriture	environment*		iam:PassRole
				proton:EnvironmentTemplate	
UpdateEnvironmentAccountConnection	Accorde l'autorisation de mettre à jour une connexion à un compte d'environnement	Écriture	environment-account-connection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEnvironmentTemplate	Accorde l'autorisation de mettre à jour un modèle d'environnement	Écrire	environment-template*		
UpdateEnvironmentTemplateMajorVersion	Accorde l'autorisation de mettre à jour une version majeure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place UpdateEnvironmentTemplateVersion	Écrire	environment-template*		
UpdateEnvironmentTemplateMinorVersion	Accorde l'autorisation de mettre à jour une version mineure d'un modèle d'environnement. OBSOLÈTE - à utiliser à la place UpdateEnvironmentTemplateVersion	Écrire	environment-template*		
UpdateEnvironmentTemplateVersion	Accorde l'autorisation de mettre à jour une version d'un modèle d'environnement	Écriture	environment-template*		
UpdateService	Accorde l'autorisation de mettre à jour un service	Écriture	service*		
				proton:ServiceTemplate	
UpdateServiceInstance	Accorde l'autorisation de mettre à jour une instance de service	Écriture	service-instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				proton:ServiceTemplate	
UpdateServicePipeline	Accorde l'autorisation de mettre à jour un pipeline de service	Écrire	service*		
				proton:ServiceTemplate	
UpdateServiceSyncBlocker	Accorde l'autorisation de mettre à jour un bloqueur de synchronisation de service	Écrire			
UpdateServiceSyncConfig	Accorde l'autorisation de mettre à jour une configuration de synchronisation de service	Écrire			
UpdateServiceTemplate	Accorde l'autorisation de mettre à jour un modèle de service	Écrire	service-template*		
UpdateServiceTemplateMajorVersion	Accorde l'autorisation de mettre à jour une version majeure d'un modèle de service. OBSOLÈTE - à utiliser à la place UpdateServiceTemplateVersion	Écrire	service-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateServiceTemplateMinorVersion	Accorde l'autorisation de créer une version mineure d'un modèle de service. OBSOLÈTE - à utiliser à la place UpdateServiceTemplateVersion	Écrire	service-template*		
UpdateServiceTemplateVersion	Accorde l'autorisation de mettre à jour une version d'un modèle de service	Écrire	service-template*		
UpdateTemplateSyncConfig	Accorde l'autorisation de mettre à jour un TemplateSyncConfig	Écrire			

Types de ressources définis par AWS Proton

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
environment-template	`arn:${Partition}:proton:${Region}:${Account}:environment-template/${Name}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
environment-template-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
environment-template-major-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
environment-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}
service-template	arn:${Partition}:proton:${Region}:${Account}:service-template/${Name}	aws:ResourceTag/${TagKey}
service-template-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
service-template-major-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
service-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}
environment	arn:${Partition}:proton:${Region}:${Account}:environment/${Name}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
service	arn:${Partition}:proton:${Region}:${Account}:service/${Name}	aws:ResourceTag/${TagKey}
service-instance	arn:${Partition}:proton:${Region}:${Account}:service/${ServiceName}/service-instance/${Name}	aws:ResourceTag/${TagKey}
environment-account-connection	arn:${Partition}:proton:${Region}:${Account}:environment-account-connection/${Id}	aws:ResourceTag/${TagKey}
repository	arn:${Partition}:proton:${Region}:${Account}:repository/${Provider}:${Name}	aws:ResourceTag/${TagKey}
component	arn:${Partition}:proton:${Region}:${Account}:component/${Id}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:proton:${Region}:${Account}:deployment/${Id}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Proton

AWS Proton définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de balise dans la requête.	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString
proton:EnvironmentTemplate	Filtre les accès par modèle d'environnement spécifié associé à la ressource	String
proton:ServiceTemplate	Filtre les accès par modèle de service spécifié associé à la ressource	String

Actions, ressources et clés de condition pour la console des bons de AWS commande

AWS La console Purchase Orders (préfixe de service :`purchase-orders`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par la console des bons de AWS commande
- Types de ressources définis par AWS Purchase Orders Console
- Clés de condition pour la console des bons de AWS commande

Actions définies par la console des bons de AWS commande

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddPurchaseOrder [autorisation uniquement]	Accorde l'autorisation d'ajouter un nouveau bon de commande	Écrire	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder [autorisation uniquement]	Accorde l'autorisation de supprimer un bon de commande	Écrire	purchase-order*		
				aws:ResourceTag/${TagKey}	
GetConsoleActionSetEnforced [autorisation uniquement]	Octroie l'autorisation de voir si des actions IAM existantes ou détaillées sont utilisées pour contrôler l'autorisation des consoles de facturation, de gestion des coûts et de compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPurchaseOrder [autorisation uniquement]	Accorde l'autorisation d'obtenir un bon de commande	Lecture	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrderInvoices [autorisation uniquement]	Accorde l'autorisation de répertorier les factures du bon de commande	List	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrders [autorisation uniquement]	Accorde l'autorisation de répertorier tous les bons de commande d'un compte	List			
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation de répertorier les balises d'un bon de commande	Lecture	purchase-order		
				aws:ResourceTag/${TagKey}	
ModifyPurchaseOrders [autorisation uniquement]	Accorde l'autorisation de modifier les bons de commande et leurs détails	Écrire	purchase-order*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TagResource [autorisation uniquement]	Accorde l'autorisation de marquer les bons de commande avec des paires de valeurs de clés données	Identification	purchase-order*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation de supprimer des balises à partir d'un bon de commande	Identification	purchase-order*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [autorisation uniquement]	Octroie l'autorisation de modifier l'utilisation ou non des actions IAM existantes ou détaillées pour contrôler l'autorisation des consoles de facturation, de gestion des coûts et de compte	Écrire			
UpdatePurchaseOrder [autorisation uniquement]	Accorde l'autorisation de mettre à jour un bon de commande existant	Écrire	purchase-order*		
				aws:ResourceTag/${TagKey}	
UpdatePurchaseOrderStatus [autorisation uniquement]	Accorde l'autorisation de définir le statut du bon de commande	Écrire	purchase-order*		
				aws:ResourceTag/${TagKey}	
ViewPurchaseOrders [autorisation uniquement]	Accorde l'autorisation d'afficher les bons de commande et les détails d'achat	Lecture	purchase-order		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS Purchase Orders Console

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
purchase-order	`arn:${Partition}:purchase-orders::${Account}:purchase-order/${ResourceName}`	aws:ResourceTag/${TagKey}

Clés de condition pour la console des bons de AWS commande

AWS La console Purchase Orders définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Q

Amazon Q (préfixe de service : q) fournit les ressources, actions et clés de contexte de condition propres au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Q
- Types de ressources définis par Amazon Q
- Clés de condition pour Amazon Q

Actions définies par Amazon Q

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateConnectorResource [autorisation uniquement]	Accorde l'autorisation d'associer une AWS ressource à un connecteur Amazon Q	Écrire			
CreateAssignment [autorisation uniquement]	Accorde l'autorisation de créer une attribution d'utilisateur ou de groupe pour un profil de développeur Amazon Q	Écrire	profile*		
				identitystore:UserId identitystore:GroupId	
CreateAuthGrant [autorisation uniquement]	Accorde l'autorisation de créer un OAuth utilisateur dans Amazon Q	Écrire			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreateOAuthAppConnection	Accorde l'autorisation d'enregistrer une OAuth application dans Amazon Q	Écrire			kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreatePlugin [autorisation uniquement]	Accorde l'autorisation de créer et de configurer un plug-in tiers dans Amazon Q	Écrire	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAssignment [autorisation uniquement]	Accorde l'autorisation de supprimer une attribution d'utilisateur ou de groupe pour un profil de développeur Amazon Q	Écrire	profile*		
				identitystore:UserId identitystore:GroupId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConversation [autorisation uniquement]	Accorde l'autorisation de supprimer une conversation avec Amazon Q	Écrire			
DeleteOAuthAppConnection [autorisation uniquement]	Accorde l'autorisation de supprimer une OAuth application dans Amazon Q	Écrire			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
DeletePlugin [autorisation uniquement]	Accorde l'autorisation de supprimer un plugin configuré dans Amazon Q	Écrire	plugin*		
				aws:ResourceTag/${TagKey}	
GenerateCodeFromCommands [autorisation uniquement]	Accorde l'autorisation de générer du code à partir de commandes CLI dans Amazon Q	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GenerateCodeRecommendations [autorisation uniquement]	Accorde l'autorisation de générer des recommandations de code dans Amazon Q	Lecture			
GetConnector [autorisation uniquement]	Autorise l'accès aux informations relatives à un connecteur Amazon Q spécifique	Lecture			
GetConversation [autorisation uniquement]	Octroie l'autorisation d'obtenir des messages individuels associés à une conversation spécifique avec Amazon Q.	Lecture			
GetIdentityMetadata [autorisation uniquement]	Autorise Amazon Q à obtenir les métadonnées d'identité	Lecture			
GetPlugin [autorisation uniquement]	Autorise l'accès aux informations relatives à un plugin Amazon Q configuré spécifique	Lecture	plugin*		
				aws:ResourceTag/${TagKey}	
GetTroubleshootingResults [autorisation uniquement]	Octroie l'autorisation d'obtenir les résultats de résolution des problèmes avec Amazon Q.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConversations [autorisation uniquement]	Accorde l'autorisation de répertorier les conversations individuelles associées à un utilisateur Amazon Q spécifique	Lecture			
ListDashboardMetrics [autorisation uniquement]	Accorde l'autorisation de lire les statistiques pour remplir le tableau de bord Amazon Q	List			
ListPluginProviders [autorisation uniquement]	Accorde l'autorisation de répertorier les plug-ins disponibles dans Amazon Q	List			
ListPlugins [autorisation uniquement]	Accorde l'autorisation de répertorier les plug-ins configurés dans Amazon Q	List	plugin*		
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation de répertorier tous les tags associés à une ressource Amazon Q	List	plugin		
				aws:ResourceTag/${TagKey}	
PassRequest [autorisation uniquement]	Accorde l'autorisation d'autoriser Amazon Q à effectuer des actions en votre nom	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RejectConnector [autorisation uniquement]	Accorde l'autorisation de rejeter une demande de connexion pour un connecteur Amazon Q	Écrire			
SendEvent [autorisation uniquement]	Accorde l'autorisation de déclencher des actions Amazon Q asynchrones	Écrire			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
SendMessage [autorisation uniquement]	Octroie l'autorisation d'envoyer un message à Amazon Q.	Écrire			
StartConversation [autorisation uniquement]	Octroie l'autorisation de démarrer une conversation avec Amazon Q.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartTroubleshootingAnalysis [autorisation uniquement]	Octroie l'autorisation de démarrer une analyse de résolution des problèmes avec Amazon Q.	Écrire			
StartTroubleshootingResolutionExplanation [autorisation uniquement]	Octroie l'autorisation de démarrer une explication de résolution des problèmes avec Amazon Q.	Écrire			
TagResource [autorisation uniquement]	Accorde l'autorisation d'associer des balises à une ressource Amazon Q	Identification	plugin		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation de supprimer les balises associées à une ressource Amazon Q	Identification	plugin		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAuthGrant [autorisation uniquement]	Accorde l'autorisation de mettre à jour OAuth l'utilisateur dans Amazon Q	Écrire			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdateConversation [autorisation uniquement]	Accorde l'autorisation de mettre à jour une conversation avec Amazon Q	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateOAuthAppConnection [autorisation uniquement]	Accorde l'autorisation de mettre à jour une OAuth application dans Amazon Q	Écrire			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdatePlugin [autorisation uniquement]	Autorise la mise à jour d'un plugin tiers dans Amazon Q	Écrire	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTroubleshootingCommandResult [autorisation uniquement]	Accorde l'autorisation de mettre à jour le résultat d'une commande de dépannage avec Amazon Q	Écrire			
UsePlugin [autorisation uniquement]	Autorise l'utilisation des plugins Amazon Q	Écrire	plugin*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
VerifyOAuthAppConnection [autorisation uniquement]	Accorde l'autorisation de vérifier une OAuth application dans Amazon Q	Écrire			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo

Types de ressources définis par Amazon Q

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
profile	`arn:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	

Types de ressources	ARN	Clés de condition
plugin	`arn:${Partition}:qdeveloper:${Region}:${Account}:plugin/${Identifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Q

Amazon Q définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource Amazon Q	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
identitystore:GroupId	Filtre l'accès par ID de groupe IAM Identity Center	ArrayOfString
identitystore:UserId	Filtre l'accès par ID d'utilisateur d'IAM Identity Center.	ArrayOfString

Actions, ressources et clés de condition pour Amazon Q Business

Amazon Q Business (préfixe de service : `qbusiness`) fournit les ressources, actions et clés de contexte de condition propres au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Q Business
- Types de ressources définis par Amazon Q Business
- Clés de condition pour Amazon Q Business

Actions définies par Amazon Q Business

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux vendus pour la ressource d'application Amazon Q Business	Gestion des autorisations	application*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociatePermission	Accorde l'autorisation d'associer une déclaration de politique basée sur les ressources à l'application	Écrire	application*		qbusiness:PutResourcePolicy
BatchDeleteDocument	Accorde l'autorisation de supprimer des documents par lots	Écrire	application*		
			index*		
BatchPutDocument	Accorde l'autorisation d'ajouter des documents par lots	Écrire	application*		
			index*		
CancelSubscription	Autorise l'annulation d'un abonnement	Écrire	application*		
			subscription*		
Chat	Octroie l'autorisation de discuter à l'aide d'une application.	Lecture	application*		
ChatSync	Octroie l'autorisation de discuter de manière synchrone à l'aide d'une application.	Lecture	application*		
CheckDocumentAccess	Accorde l'autorisation de vérifier si un utilisateur a accès à un document	Lecture	application*		
			index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAnonymousWebExperienceUrl	Autorise la création d'une URL unique pour une expérience Web anonyme sur Amazon Q Business	Écrire	application*		
			web-experience*		
CreateApplication	Accorde l'autorisation de créer une application	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateChatResponseConfiguration	Accorde l'autorisation de créer une configuration de réponse au chat à l'application	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessor	Accorde l'autorisation de créer DataAccessor à l'application	Écrire	application*		qbusiness:CreateDataAccessorWithTti

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessorWithTti [autorisation uniquement]	Accorde l'autorisation de créer un émetteur de jetons de confiance du centre d'identité AWS IAM basé sur DataAccessor l'application	Écrire	application*		
CreateDataSource	Octroie l'autorisation de créer une source de données pour une application et un index donnés.	Écrire	application*		
			index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Octroie l'autorisation de créer un index pour une application donnée.	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegration	Accorde l'autorisation de créer une nouvelle intégration pour une application Q Business	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlugin	Octroie l'autorisation de créer un plug-in pour une application donnée.	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetriever	Octroie l'autorisation de créer un extracteur pour une application donnée.	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Accorde l'autorisation de créer un abonnement	Écrire	application*		
				identitystore:UserId identitystore:GroupId	
CreateUser	Accorde l'autorisation de créer un utilisateur	Écrire	application*		
CreateWebExperience	Octroie l'autorisation de créer une expérience Web pour une application donnée.	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Accorde l'autorisation de supprimer une application	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAttachment	Accorde l'autorisation de supprimer une pièce jointe dans le contexte de discussion actuel	Écrire	application*		
DeleteChatControlsConfiguration	Octroie l'autorisation de supprimer une configuration de contrôles de chat pour une application.	Écrire	application*		
DeleteChatResponseConfiguration	Autorise la suppression d'une configuration de réponse au chat	Écrire	application*		
			chat-response-configuration*		
DeleteConversation	Octroie l'autorisation de supprimer une conversation.	Écrire	application*		
DeleteDataAccessor	Accorde l'autorisation de suppression DataAccessor	Écrire	application*		
			data-accessor*		
DeleteDataSource	Accorde l'autorisation de supprimer un DataSource	Écrire	application*		
			data-source*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			index*		
DeleteGroup	Accorde l'autorisation de supprimer un groupe	Écrire	application*		
			index*		
DeleteIndex	Octroie l'autorisation de supprimer un index.	Écrire	application*		
			index*		
DeleteIntegration	Accorde l'autorisation de supprimer une intégration pour une application Q Business	Écrire	application*		
			integration*		
DeletePlugin	Octroie l'autorisation de supprimer un plug-in.	Écrire	application*		
			plugin*		
DeleteRetriever	Octroie l'autorisation de supprimer un extracteur.	Écrire	application*		
			retriever*		
DeleteUser	Accorde l'autorisation de supprimer un utilisateur	Écrire	application*		
DeleteWebExperience	Octroie l'autorisation de supprimer une expérience Web.	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			web-experience*		
DisableAclOnDataSource [autorisation uniquement]	Accorde l'autorisation de désactiver l'analyse ACL lors de la création de la ressource de source de données Amazon Q Business	Écrire	application*		
DisassociatePermission	Accorde l'autorisation de dissocier la déclaration de politique basée sur les ressources de l'application	Écrire	application*		qbusiness:PutResourcePolicy
GetApplication	Accorde l'autorisation d'obtenir une application	Lecture	application*		
GetChatControlsConfiguration	Octroie l'autorisation d'obtenir une configuration de contrôles de chat pour une application.	List	application*		
GetChatResponseConfiguration	Accorde l'autorisation d'obtenir une configuration de réponse au chat	Lecture	application*		
			chat-response-configuration*		
GetDataAccessor	Donne l'autorisation d'obtenir DataAccessor	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			data-accessor*		
GetDataSource	Octroie l'autorisation d'obtenir une source de données.	Lecture	application*		
			data-source*		
			index*		
GetDocumentContent	Accorde l'autorisation d'obtenir le contenu d'un document	Lecture	application*		
			index*		
GetGroup	Octroie l'autorisation d'obtenir un groupe.	Lecture	application*		
			index*		
GetIndex	Octroie l'autorisation d'obtenir un index.	Lecture	application*		
			index*		
GetIntegration	Accorde l'autorisation d'obtenir une intégration pour une application Q Business	Lecture	application*		
			integration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMedia	Accorde l'autorisation d'obtenir le média associé à un message système	Lecture	application*		
GetPlugin	Octroie l'autorisation d'obtenir un plug-in.	Lecture	application*		
			plugin*		
GetPolicy	Accorde l'autorisation d'obtenir la politique basée sur les ressources de l'application	Lecture	application*		
GetRetriever	Octroie l'autorisation d'obtenir un extracteur.	Lecture	application*		
			retriever*		
GetUser	Octroie l'autorisation d'obtenir un utilisateur.	Lecture	application*		
GetWebExperience	Octroie l'autorisation d'obtenir une expérience Web.	Lecture	application*		
			web-experience*		
ListApplications	Octroie l'autorisation de répertorier les applications.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAttachments	Accorde l'autorisation de répertorier les pièces jointes dans le contexte de discussion actuel	List	application*		
ListChatResponseConfigurations	Accorde l'autorisation de répertorier les configurations de réponse au chat pour une application	List	application*		
ListConversations	Octroie l'autorisation de répertorier toutes les conversations d'une application.	List	application*		
ListDataAccessors	Accorde l'autorisation de créer DataAccessors une liste pour l'application	List	application*		
ListDataSourceSyncJobs	Accorde l'autorisation d'obtenir l'historique des tâches de synchronisation des sources de données	List	application*		
			data-source*		
			index*		
ListDataSources	Octroie l'autorisation de répertorier les sources de données d'une application et d'un index.	List	application*		
			index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDocuments	Octroie l'autorisation de répertorier tous les documents.	List	application*		
			index*		
ListGroups	Accorde l'autorisation de répertorier des groupes	List	application*		
			index*		
ListIndices	Octroie l'autorisation de répertorier les index d'une application.	List	application*		
ListIntegrations	Permet de répertorier toutes les intégrations pour une application Q Business	List	application*		
ListMessages	Octroie l'autorisation de répertorier tous les messages.	List	application*		
ListPluginActions	Accorde l'autorisation de répertorier les actions d'un plugin dans l'application	Lecture	application*		
			plugin*		
ListPluginTypeActions	Accorde l'autorisation de répertorier toutes les actions pour un type de plugin	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPluginTypeMetadata	Accorde l'autorisation de répertorier toutes les métadonnées du type de plugin	Lecture			
ListPlugins	Octroie l'autorisation de répertorier les plug-ins d'une application.	List	application*		
ListRetrievers	Octroie l'autorisation de répertorier les extracteurs d'une application.	List	application*		
ListSubscriptions	Accorde l'autorisation de répertorier les abonnements	List	application*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			integration		
			plugin		
			retriever		
			web-experience		
ListWebExperiences	Octroie l'autorisation de répertorier les expériences Web d'une application.	List	application*		
PutFeedback	Octroie l'autorisation de saisir des commentaires concernant un message de conversation.	Écrire	application*		
PutGroup	Octroie l'autorisation de saisir un groupe d'utilisateurs.	Écrire	application*		
			index*		
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation d'ajouter une déclaration de politique basée sur les ressources à l'application	Écrire	application*		
SearchRelevantContent	Accorde l'autorisation de rechercher du contenu pertinent à partir de l'application Amazon Q Business	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDataSourceSyncJob	Accorde l'autorisation de démarrer la tâche de synchronisation des sources de données	Écrire	application*		
			data-source*		
			index*		
StartDeployment	Accorde l'autorisation de démarrer le déploiement d'une intégration	Écrire	application*		
			integration*		
StopDataSourceSyncJob	Accorde l'autorisation d'arrêter la tâche de synchronisation des sources de données	Écrire	application*		
			data-source*		
			index*		
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Identification	application		
			chat-response-configuration		
			data-accessor		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer la balise avec la clé donnée d'une ressource	Identification	application		
			chat-response-configuration		
			data-accessor		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
				aws:TagKeys	
UpdateApplication	Octroie l'autorisation de mettre à jour une application.	Écrire	application*		
UpdateChatControlsConfiguration	Octroie l'autorisation de mettre à jour une configuration de contrôles de chat pour une application.	Écrire	application*		
UpdateChatResponseConfiguration	Accorde l'autorisation de mettre à jour la configuration d'une réponse au chat	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			chat-response-configuration*		
UpdateDataAccessor	Accorde l'autorisation de mise à jour DataAccessor	Écrire	application*		
			data-accessor*		
UpdateDataSource	Accorde l'autorisation de mettre à jour un DataSource	Écrire	application*		
			data-source*		
			index*		
UpdateIndex	Octroie l'autorisation de mettre à jour un index.	Écrire	application*		
			index*		
UpdateIntegration	Autorise la mise à jour d'une intégration pour une application Q Business	Écrire	application*		
			integration*		
UpdatePlugin	Octroie l'autorisation de mettre à jour un plug-in.	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			plugin*		
UpdateRetriever	Octroie l'autorisation de mettre à jour un extracteur.	Écrire	application*		
			retriever*		
UpdateSubscription	Autorise la mise à jour d'un abonnement	Écrire	application*		
			subscription*		
UpdateUser	Octroie l'autorisation de mettre à jour un utilisateur.	Écrire	application*		
UpdateWebExperience	Accorde l'autorisation de mettre à jour un WebExperience	Écrire	application*		
			web-experience*		

Types de ressources définis par Amazon Q Business

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/integration/${IntegrationId}	aws:ResourceTag/${TagKey}
retriever	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/retriever/${RetrieverId}	aws:ResourceTag/${TagKey}
index	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}	aws:ResourceTag/${TagKey}
data-source	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}/data-source/${DataSourceId}	aws:ResourceTag/${TagKey}
plugin	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/plugin/${PluginId}	aws:ResourceTag/${TagKey}
web-experience	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/web-experience/${WebExperienceId}	aws:ResourceTag/${TagKey}
subscription	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/subscription/${SubscriptionId}	

Types de ressources	ARN	Clés de condition
data-accessor	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/data-accessor/${DataAccessorId}`	aws:ResourceTag/${TagKey}
chat-response-configuration	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/chat-response-configuration/${ChatResponseConfigurationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Q Business

Amazon Q Business définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
identitystore:GroupId	Filtre l'accès par ID de groupe IAM Identity Center	ArrayOfString

Clés de condition	Description	Type
identitystore:UserId	Filtre l'accès par ID d'utilisateur d'IAM Identity Center.	ArrayOfString

Actions, ressources et clés de condition pour les applications Amazon Q Business Q

Amazon Q Business Q Apps (préfixe de service :`qapps`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Q Business Q Apps
- Types de ressources définis par Amazon Q Business Q Apps
- Clés de condition pour les applications Amazon Q Business Q

Actions définies par Amazon Q Business Q Apps

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateLibraryItemReview	Accorde l'autorisation d'associer une revue d'éléments de bibliothèque dans l'environnement d'application Q Business	Écrire	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
AssociateQAppWithUser	Accorde l'autorisation d'associer Q App à un utilisateur dans l'environnement d'applications Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
BatchCreateCategory	Accorde l'autorisation de créer les catégories d'une bibliothèque dans l'environnement d'application Q Business	Écrire	application*		
BatchDeleteCategory	Accorde l'autorisation de supprimer les catégories d'une bibliothèque dans	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	l'environnement d'application Q Business				
BatchUpdateCategory	Autorise la mise à jour des catégories d'une bibliothèque dans l'environnement d'application Q Business	Écrire	application*		
CopyQApp [autorisation uniquement]	Autorise la copie de Q App dans l'environnement d'applications Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateLibraryItem	Accorde l'autorisation de créer un élément de bibliothèque dans l'environnement d'application Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateLibraryItemReview [autorisation uniquement]	Accorde l'autorisation de créer une revue d'éléments de bibliothèque dans l'environnement d'application Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateQApp	Accorde l'autorisation de créer une application Q dans l'environnement d'applications Q Business	Écrire	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionToken [autorisation uniquement]	Accorde l'autorisation de s'abonner à une rubrique du bus d'événements Q App dans l'environnement d'application Q Business	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLibraryItem	Accorde l'autorisation de supprimer un élément de bibliothèque dans l'environnement d'application Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DeleteQApp	Autorise la suppression de Q App dans l'environnement d'applications Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DescribeQAppPermissions	Accorde l'autorisation d'obtenir des autorisations de partage de Q App dans l'environnement d'applications Q Business	Lecture	application		
			qapp		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateLibraryItemReview	Accorde l'autorisation de dissocier la révision d'un élément de bibliothèque dans l'environnement d'application Q Business	Écrire	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateQAppFromUser	Accorde l'autorisation de dissocier Q App d'un utilisateur dans l'environnement d'applications Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportQAppSessionData	Accorde l'autorisation d'exporter les données de session Q App dans l'environnement d'application Q Business	Écrire	qapp-session*		
GetLibraryItem	Accorde l'autorisation d'obtenir un élément de bibliothèque dans l'environnement d'application Q Business	Lecture	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQApp	Accorde l'autorisation d'obtenir Q App dans l'environnement d'applications Q Business	Lecture	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQAppSession	Accorde l'autorisation d'obtenir une session Q App dans l'environnement d'application Q Business	Lecture	qapp-session*		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
GetQAppSessionMetadata	Accorde l'autorisation d'obtenir les métadonnées de session Q App dans l'environnement d'application Q Business	Lecture	qapp-session*		
ImportDocument	Accorde l'autorisation d'importer un document dans Q App ou Q App Session dans l'environnement d'application Q Business	Écrire	qapp		
			qapp-session		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
ListCategories	Accorde l'autorisation de répertorier les catégories dans l'environnement d'application Q Business	List	application*		
ListLibraryItems	Accorde l'autorisation de répertorier les éléments de bibliothèque dans l'environnement d'application Q Business	List	application*		
ListQAppSessionData	Accorde l'autorisation d'obtenir les données de session Q App dans l'environnement d'application Q Business	Lecture	qapp-session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListQApps	Accorde l'autorisation de répertorier les applications Q dans l'environnement d'applications Q Business	List	application*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	qapp		
			qapp-session		
PredictProblemStatementFromConversation [autorisation uniquement]	Autorise à prédire l'énoncé du problème à partir du journal des conversations dans l'environnement d'application Q Business	Écrire	application*		
PredictQApp	Accorde l'autorisation de prédire Q App à partir du journal des conversations ou de l'énoncé du problème dans l'environnement d'application Q Business	Écrire	application*		
PredictQAppFromProblemStatement [autorisation uniquement]	Accorde l'autorisation de prédire les métadonnées de Q App à partir de l'énoncé du problème dans l'environnement d'application Q Business	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartQAppSession	Accorde l'autorisation de démarrer une session Q App dans l'environnement d'application Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished aws:RequestTag/${TagKey} aws:TagKeys	
StopQAppSession	Autorise l'arrêt de la session Q App dans l'environnement applicatif Q Business	Écrire	application		
			qapp-session		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Identification	qapp		
			qapp-session		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer la balise avec la clé donnée d'une ressource	Identification	qapp		
			qapp-session		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateLibraryItem	Accorde l'autorisation de mettre à jour un élément de bibliothèque dans l'environnement d'application Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateLibraryItemMetadata	Accorde l'autorisation de mettre à jour les métadonnées d'un élément de bibliothèque dans l'environnement d'application Q Business	Écrire	qapp*		
				qapps:AppIsPublished	
UpdateQApp	Autorise la mise à jour de Q App dans l'environnement d'applications Q Business	Écrire	application		
			qapp		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateQAppPermissions	Accorde l'autorisation de mettre à jour les autorisations de partage de Q App dans l'environnement d'applications Q Business	Écrire	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateQAppSession	Accorde l'autorisation de mettre à jour la session Q App dans l'environnement d'application Q Business	Écrire	qapp-session*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
UpdateQAppSessionMetadata	Accorde l'autorisation de mettre à jour les métadonnées de session Q App dans l'environnement d'application Q Business	Écrire	qapp-session*		

Types de ressources définis par Amazon Q Business Q Apps

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	
qapp	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}`	aws:ResourceTag/${TagKey}
qapp-session	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}/session/${SessionId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les applications Amazon Q Business Q

Amazon Q Business Q Apps définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Clés de condition	Description	Type
qapps:AppIsPublished	Filtre l'accès en fonction de la publication de Q App	String
qapps:SessionIsShared	Filtre l'accès en fonction du partage ou non de Q App Session	String
qapps:UserIsAppOwner	Filtre l'accès selon que le demandeur est propriétaire de l'application Q	String
qapps:UserIsSessionModerator	Filtre l'accès selon que le demandeur est le modérateur de Q App Session	String

Actions, ressources et clés de condition pour Amazon Q Developer

Amazon Q Developer (préfixe de service :`qdeveloper`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Q Developer
- Types de ressources définis par Amazon Q Developer
- Clés de condition pour Amazon Q Developer

Actions définies par Amazon Q Developer

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportArtifact	Accorde l'autorisation d'exporter des artefacts depuis Amazon Q Developer	Écrire	codeTransformation		
ImportArtifact	Accorde l'autorisation d'importer des artefacts à Amazon Q Developer	Écrire	codeTransformation		
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation de répertorier tous les tags associés à une ressource Amazon Q Developer	List	codeTransformation		
StartAgentSession	Accorde l'autorisation de démarrer une session d'agent avec Amazon Q Developer	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [autorisation uniquement]	Accorde l'autorisation d'associer des balises à une ressource Amazon Q Developer	Identification	codeTransformation		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TransformCode	Autorise la transformation du code avec Amazon Q Developer Transform Agent	Écrire	codeTransformation		
UntagResource [autorisation uniquement]	Accorde l'autorisation de supprimer les balises associées à une ressource Amazon Q Developer	Identification	codeTransformation		
				aws:TagKeys	

Types de ressources définis par Amazon Q Developer

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
codeTransformation	`arn:${Partition}:qdeveloper:${Region}:${Account}:codeTransformation/${Identifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Q Developer

Amazon Q Developer définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource Amazon Q Developer	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Q in Connect

Amazon Q in Connect (préfixe de service : `wisdom`) fournit les ressources, actions et clés de contexte de condition propres au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Q in Connect
- Types de ressources définis par Amazon Q in Connect
- Clés de condition pour Amazon Q in Connect

Actions définies par Amazon Q in Connect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateMessageTemplate	Accorde l'autorisation d'activer un modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux vendus à un assistant	Gestion des autorisations	Assistant		
CreateAIAgent	Accorde l'autorisation de créer un agent d'intelligence artificielle	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIAgentVersion	Accorde l'autorisation de créer une version de l'agent AI	Écrire	AIAgent*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey}	
CreateAIGuardrail	Autorise la création d'un garde-corps antiaérien	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrailVersion	Autorise la création d'une version AI Guardrail	Écrire	AIGuardrail*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPrompt	Accorde l'autorisation de créer une invite AI	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPromptVersion	Accorde l'autorisation de créer une version AI prompt	Écrire	AIPrompt*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistant	Accorde l'autorisation de créer un assistant	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistantAssociation	Accorde l'autorisation de créer une association entre un assistant et une autre ressource	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateContent	Accorde l'autorisation de créer du contenu	Écrire	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
	Accorde l'autorisation de créer une association de contenu	Écrire	Content*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateContentAssociation			KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKnowledgeBase	Accorde l'autorisation de créer une base de connaissances	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplate	Accorde l'autorisation de créer un modèle de message	Écrire	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplateAttachment	Accorde l'autorisation de créer une pièce jointe à un modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMessageTemplateVersion	Accorde l'autorisation de créer une version d'un modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		
CreateQuickResponse	Accorde l'autorisation de créer une réponse rapide	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSession	Accorde l'autorisation de créer une session	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMessageTemplate	Accorde l'autorisation de désactiver un modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		
DeleteAIAgent	Accorde l'autorisation de supprimer un agent d'intelligence artificielle	Écrire	AIAgent*		
DeleteAIAgentVersion	Autorise la suppression d'une version d'un agent AI	Écrire	AIAgent*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAIGuardrail	Autorise la suppression d'un garde-corps aérien	Écrire	AIGuardrail*		
DeleteAIGuardrailVersion	Autorise la suppression d'une version d'AI Guardrail	Écrire	AIGuardrail*		
DeleteAIPrompt	Autorise la suppression d'une invite AI	Écrire	AIPrompt*		
DeleteAIPromptVersion	Autorise la suppression d'une version d'AI prompt	Écrire	AIPrompt*		
DeleteAssistant	Accorde l'autorisation de supprimer un assistant	Écrire	Assistant*		
DeleteAssistantAssociation	Accorde l'autorisation de supprimer une association d'assistant	Écrire	AssistantAssociation*		
DeleteContent	Accorde l'autorisation de supprimer du contenu	Écrire	Content*		
			KnowledgeBase*		
DeleteContentAssociation	Accorde l'autorisation de supprimer une association de contenu	Écrire	Content*		
			ContentAssociation*		
			KnowledgeBase*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteImportJob	Accorde l'autorisation de supprimer une tâche d'importation d'une base de connaissances	Écrire	KnowledgeBase*		
DeleteKnowledgeBase	Accorde l'autorisation de supprimer une base de connaissances	Écrire	KnowledgeBase*		
DeleteMessageTemplate	Accorde l'autorisation de supprimer un modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		
DeleteMessageTemplateAttachment	Autorise la suppression d'une pièce jointe d'un modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		
DeleteQuickResponse	Accorde l'autorisation de supprimer une réponse rapide	Écrire	KnowledgeBase*		
			QuickResponse*		
GetAIAgent	Accorde l'autorisation de récupérer des informations sur un agent d'intelligence artificielle	Lecture	AIAgent*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAIGuardrail	Donne l'autorisation de récupérer des informations sur un garde-corps antiaérien	Lecture	AIGuardrail*		
GetAIPrompt	Accorde l'autorisation de récupérer des informations sur une invite AI	Lecture	AIPrompt*		
GetAssistant	Accorde l'autorisation de récupérer les informations sur un assistant	Lecture	Assistant*		
GetAssistantAssociation	Accorde l'autorisation de récupérer les informations sur une association d'assistant	Lecture	AssistantAssociation*		
GetContent	Accorde l'autorisation de récupérer du contenu, y compris une URL présignée pour télécharger le contenu	Lecture	Content*		
			KnowledgeBase*		
GetContentAssociation	Accorde l'autorisation de récupérer des informations sur une association de contenu	Lecture	Content*		
			ContentAssociation*		
			KnowledgeBase*		
GetContentSummary	Accorde l'autorisation de récupérer des informations récapitulatives sur du contenu	Lecture	Content*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			KnowledgeBase*		
GetImportJob	Accorde l'autorisation de récupérer des informations sur une tâche d'importation	Lecture	KnowledgeBase*		
GetKnowledgeBase	Accorde l'autorisation de récupérer des informations sur la base de connaissances	Lecture	KnowledgeBase*		
GetMessageTemplate	Accorde l'autorisation de récupérer un modèle de message	Lecture	KnowledgeBase*		
			MessageTemplate*		
				wisdom:MessageTemplate/RoutingProfileArn	
GetNextMessage	Accorde l'autorisation de récupérer le message suivant d'une session	Lecture	Session*		
GetQuickResponse	Accorde l'autorisation d'extraire du contenu	Lecture	KnowledgeBase*		
			QuickResponse*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRecommendations	Accorde l'autorisation de récupérer des recommandations pour la session spécifiée	Lecture	Session*		
GetSession	Accorde l'autorisation de récupérer des informations pour une session spécifiée	Lecture	Session*		
ListAIAgentVersions	Accorde l'autorisation de répertorier des informations sur les versions de l'agent AI	List	AIAgent*		
ListAIAgents	Accorde l'autorisation de répertorier des informations sur les agents de l'IA	List			
ListAIGuardrailVersions	Accorde l'autorisation de répertorier des informations sur les versions d'AI Guardrail	List	AIGuardrail*		
ListAIGuardrails	Autorise à répertorier des informations sur les garde-corps aériens	List			
ListAIPromptVersions	Accorde l'autorisation de répertorier des informations sur les versions d'ai prompt	List	AIPrompt*		
ListAIPrompts	Accorde l'autorisation de répertorier des informations sur les invites AI	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAssistantAssociations	Accorde l'autorisation de répertorier des informations sur des associations d'assistant	List			
ListAssistants	Accorde l'autorisation de répertorier des informations sur les assistants	List			
ListContentAssociations	Accorde l'autorisation de répertorier les informations relatives aux associations de contenus	List	Content* KnowledgeBase*		
ListContents	Accorde l'autorisation de répertorier le contenu avec une base de connaissances	List	KnowledgeBase*		
ListImportJobs	Accorde l'autorisation de récupérer des informations sur des bases de connaissances	List	KnowledgeBase*		
ListKnowledgeBases	Accorde l'autorisation de récupérer des informations sur des bases de connaissances	List			
ListMessageTemplateVersions	Accorde l'autorisation de répertorier les versions du modèle de message pour le modèle de message spécifié	List	KnowledgeBase* MessageTemplate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMessageTemplates	Accorde l'autorisation de répertorier les modèles de messages pour une base de connaissances	List	KnowledgeBase*		
ListMessages	Accorde l'autorisation de répertorier les messages dans une session	List	Session*		
ListQuickResponses	Accorde l'autorisation de répertorier une réponse rapide dans une base de connaissances	List	KnowledgeBase*		
ListTagsForResource	Accorde l'autorisation de répertorier des balises pour la ressource spécifiée	Lecture			
NotifyRecommendationsReceived	Accorde l'autorisation de supprimer les recommandations spécifiées de la file d'attente des recommandations nouvellement disponibles de l'assistant spécifié	Écrire	Session*		
PutFeedback	Accorde l'autorisation de soumettre des commentaires	Écrire	Assistant*		
QueryAssistant	Accorde l'autorisation d'effectuer une recherche manuelle avec l'assistant spécifié	Lecture	Assistant*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveAssistantAIAgent	Accorde l'autorisation de supprimer un agent AI d'un assistant	Écrire	Assistant*		
RemoveKnowledgeBaseTemplateUri	Accorde l'autorisation de supprimer un modèle d'URI d'une base de connaissances	Écrire	KnowledgeBase*		
RenderMessageTemplate	Accorde l'autorisation d'afficher un modèle de message	Lecture	KnowledgeBase*		wisdom:GetMessageTemplate
			MessageTemplate*		
				wisdom:MessageTemplate/RoutingProfileArn	
Retrieve	Accorde l'autorisation de récupérer le contenu des connaissances auprès d'associations d'assistants spécifiées	Lecture	Assistant*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchContent	Accorde l'autorisation de rechercher du contenu référençant une base de connaissances spécifiée. Peut être utilisé pour obtenir une ressource de contenu spécifique par son nom	Lecture	KnowledgeBase*		
SearchMessageTemplates	Accorde l'autorisation de rechercher des modèles de messages faisant référence à une base de connaissances spécifiée	Lecture	KnowledgeBase*		
				wisdom:SearchFilter/RoutingProfileArn wisdom:SearchFilter/Qualifier	
SearchQuickResponses	Accorde l'autorisation de rechercher une réponse rapide en se référant à une base de connaissances spécifiée	Lecture	KnowledgeBase*		wisdom:GetQuickResponse
				wisdom:SearchFilter/RoutingProfileArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchSessions	Accorde l'autorisation de rechercher des sessions référençant un assistant spécifié. Peut être utilisé pour définir une ressource de session spécifique par son nom	Lecture			
SendMessage	Accorde l'autorisation d'envoyer un message	Écrire	Session*		
StartContentUpload	Accorde l'autorisation d'obtenir une URL pour charger du contenu dans une base de connaissances	Écrire	KnowledgeBase*		
StartImportJob	Accorde l'autorisation de créer plusieurs réponses rapides	Écrire	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Accorde l'autorisation d'ajouter les balises spécifiées à la ressource spécifiée	Identification	Assistant		
			AssistantAssociation		
			Content		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les balises spécifiées de la ressource spécifiée	Identification	Assistant		
			AssistantAssociation		
			Content		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ContentAssociation		
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAIAgent	Accorde l'autorisation de mettre à jour les informations relatives à un agent d'intelligence artificielle	Écrire	AIAgent*		
UpdateAIGuardrail	Accorde l'autorisation de mettre à jour les informations relatives à un garde-corps à air comprimé	Écrire	AIGuardrail*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAIPrompt	Autorise la mise à jour des informations relatives à une invite AI	Écrire	AIPrompt*		
UpdateAssistantAIAgent	Accorde l'autorisation de mettre à jour les informations d'un assistant concernant un agent d'intelligence artificielle	Écrire	Assistant*		
UpdateContent	Accorde l'autorisation de mettre à jour les informations sur le contenu	Écrire	Content*		
			KnowledgeBase*		
UpdateKnowledgeBaseTemplateUri	Accorde l'autorisation de mettre à jour l'URI du modèle d'une base de connaissances	Écrire	KnowledgeBase*		
UpdateMessageTemplate	Autorise la mise à jour du contenu du modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		
UpdateMessageTemplateMetadata	Autorise la mise à jour des métadonnées du modèle de message	Écrire	KnowledgeBase*		
			MessageTemplate*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateQuickResponse	Accorde l'autorisation de mettre à jour les informations ou le contenu de la réponse rapide	Écrire	KnowledgeBase*		
			QuickResponse*		
UpdateSession	Accorde l'autorisation de mettre à jour une session	Écrire	Session*		
UpdateSessionData	Autorise la mise à jour des données stockées dans une session	Écrire	Session*		

Types de ressources définis par Amazon Q in Connect

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AIAgent	`arn:${Partition}:wisdom:${Region}:${Account}:ai-agent/${AssistantId}/${AIAgentId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
AIPrompt	arn:${Partition}:wisdom:${Region}:${Account}:ai-prompt/${AssistantId}/${AIPromptId}	aws:ResourceTag/${TagKey}
AIGuardrail	arn:${Partition}:wisdom:${Region}:${Account}:ai-guardrail/${AssistantId}/${AIGuardrailId}	aws:ResourceTag/${TagKey}
Assistant	arn:${Partition}:wisdom:${Region}:${Account}:assistant/${AssistantId}	aws:ResourceTag/${TagKey}
Assistant Association	arn:${Partition}:wisdom:${Region}:${Account}:association/${AssistantId}/${AssistantAssociationId}	aws:ResourceTag/${TagKey}
Content	arn:${Partition}:wisdom:${Region}:${Account}:content/${KnowledgeBaseId}/${ContentId}	aws:ResourceTag/${TagKey}
ContentAssociation	arn:${Partition}:wisdom:${Region}:${Account}:content-association/${KnowledgeBaseId}/${ContentId}/${ContentAssociationId}	aws:ResourceTag/${TagKey}
KnowledgeBase	arn:${Partition}:wisdom:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
MessageTemplate	arn:${Partition}:wisdom:${Region}:${Account}:message-template/${KnowledgeBaseId}/${MessageTemplateId}	aws:ResourceTag/${TagKey} wisdom:MessageTemplate/RoutingProfileArn

Types de ressources	ARN	Clés de condition
Session	`arn:${Partition}:wisdom:${Region}:${Account}:session/${AssistantId}/${SessionId}`	aws:ResourceTag/${TagKey}
QuickResponse	`arn:${Partition}:wisdom:${Region}:${Account}:quick-response/${KnowledgeBaseId}/${QuickResponseId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Q in Connect

Amazon Q in Connect définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
wisdom:MessageTemplate/RoutingProfileArn	Filtre l'accès en fonction des arns du profil de routage Connect associés à la ressource	ArrayOfARN

Clés de condition	Description	Type
wisdom:SearchFilter/Qualifier	Filtre l'accès en fonction des qualificatifs transmis dans la demande	ArrayOfString
wisdom:SearchFilter/RoutingProfileArn	Filtre l'accès par le profil de routage connect arn qui est transmis dans la demande	ARN

Actions, ressources et clés de condition pour Amazon QLDB

Amazon QLDB (préfixe de service : `qldb`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon QLDB
- Types de ressources définis par Amazon QLDB
- Clés de condition pour Amazon QLDB

Actions définies par Amazon QLDB

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelJournalKinesisStream	Accorde l'autorisation d'annuler un flux Kinesis de journal	Écriture	stream*		
CreateLedger	Accorde l'autorisation de créer un registre.	Écriture	ledger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLedger	Accorde l'autorisation de supprimer un registre.	Écriture	ledger*		
DescribeJournalKinesisStream	Accorde l'autorisation de décrire des informations sur un flux Kinesis de journal	Lecture	stream*		
DescribeJournalS3Export	Accorde l'autorisation de décrire des informations sur une tâche d'exportation de journal	Lecture	ledger*		
DescribeLedger	Accorde l'autorisation de décrire un registre.	Lecture	ledger*		
ExecuteStatement [autorisation uniquement]	Accorde l'autorisation d'envoyer des commandes à un registre via la console	Écriture	ledger*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportJournalToS3	Accorde l'autorisation d'exporter le contenu du journal vers un compartiment Amazon S3	Écrire	ledger*		
GetBlock	Accorde l'autorisation de récupérer un bloc d'un registre pour une donnée BlockAddress	Lecture	ledger*		
GetDigest	Accorde l'autorisation de récupérer un résumé d'un registre pour une donnée BlockAddress	Lecture	ledger*		
GetRevision	Accorde l'autorisation de récupérer une révision pour un identifiant de document donné et un numéro donné BlockAddress	Lecture	ledger*		
InsertSampleData [autorisation uniquement]	Accorde l'autorisation d'insérer des exemples de données d'application via la console	Écriture	ledger*		
ListJournalKinesisStreamsForLedger	Accorde l'autorisation de répertorier les flux Kinesis de journal pour un registre spécifié	Liste	stream*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListJournalS3Exports	Accorde l'autorisation de répertorier les tâches d'exportation de journal pour tous les registres	Liste			
ListJournalS3ExportsForLedger	Accorde l'autorisation de répertorier les tâches d'exportation de journal pour un registre spécifié	Liste	ledger*		
ListLedgers	Accorde l'autorisation de répertorier les registres existants	Liste			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	catalog		
			ledger		
			stream		
			table		
PartiQLCreateIndex	Accorde l'autorisation de créer un index sur une table	Écriture	table*		
PartiQLCreateTable	Accorde l'autorisation de créer une table.	Écriture	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PartiQLDelete	Accorde l'autorisation de supprimer des documents d'une table	Écriture	table*		
PartiQLDropIndex	Accorde l'autorisation de supprimer un index d'une table	Écriture	table*		
				qldb:Purge	
PartiQLDropTable	Accorde l'autorisation de supprimer une table	Écriture	table*		
				qldb:Purge	
PartiQLHistoryFunction	Accorde l'autorisation d'utiliser la fonction d'historique sur une table	Lecture	table*		
PartiQLInsert	Accorde l'autorisation d'insérer des documents dans une table	Écrire	table*		
PartiQLRedact	Accorde l'autorisation de censurer des révisions historiques	Écrire	table*		
PartiQLSelect	Accorde l'autorisation de sélectionner des documents à partir d'une table	Lecture	catalog		
			table		
PartiQLUndropTable	Accorde l'autorisation d'annuler la suppression d'une table	Écriture	table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PartiQLUpdate	Accorde l'autorisation de mettre à jour des documents existants dans une table	Écriture	table*		
SendCommand	Accorde l'autorisation d'envoyer des commandes à un registre	Écrire	ledger*		
ShowCatalog [autorisation uniquement]	Accorde l'autorisation d'afficher le catalogue d'un registre via la console	Écriture	ledger*		
StreamJournalToKinesis	Octroie l'autorisation de diffuser le contenu du journal vers un flux de données Kinesis	Écriture	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une ressource	Balisage	catalog		
			ledger		
			stream		
			table		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Balisage	catalog		
			ledger		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateLedger	Accorde l'autorisation de mettre à jour les propriétés d'un registre	Écriture	ledger*		
UpdateLedgerPermissionsMode	Accorde l'autorisation de mettre à jour le mode d'autorisations sur un registre	Écriture	ledger*		

Types de ressources définis par Amazon QLDB

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
ledger	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:qldb:${Region}:${Account}:stream/${LedgerName}/${StreamId}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/table/${TableId}`	aws:ResourceTag/${TagKey}
catalog	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/information_schema/user_tables`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon QLDB

Amazon QLDB définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d’application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
qldb:Purge	Filtre l'accès en fonction de la valeur de purge spécifiée dans une instruction DROP PartiQL	String

Actions, ressources et clés de condition pour Amazon QuickSight

Amazon QuickSight (préfixe de service :`quicksight`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon QuickSight
- Types de ressources définis par Amazon QuickSight
- Clés de condition pour Amazon QuickSight

Actions définies par Amazon QuickSight

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AccountConfigurations [autorisation uniquement]	Accorde l'autorisation d'activer la définition de l'accès par défaut aux AWS ressources	Écrire			
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux, QuickSuite par exemple	Gestion des autorisations			
BatchCreateTopicReviewedAnswer	Accorde l'autorisation de créer des réponses révisées pour un sujet	Écrire	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchDeleteTopicReviewedAnswer	Accorde l'autorisation de supprimer les réponses révisées pour un sujet	Écrire	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetPreferences [autorisation uniquement]	Accorde l'autorisation d'obtenir les préférences de l'utilisateur	Lecture			
BatchUpdatePreferences [autorisation uniquement]	Accorde l'autorisation de mettre à jour les préférences de l'utilisateur	Écrire			
CancelIngestion	Accorde l'autorisation d'annuler une ingestion SPICE sur un jeu de données.	Écrire	ingestion *		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountCustomization	Accorde l'autorisation de créer une personnalisation de compte pour le QuickSight compte ou l'espace de noms	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAccountSubscription	Accorde l'autorisation de s'abonner à QuickSight	Écrire		quicksight:Edition quicksight:DirectoryType	
CreateActionConnector	Accorde l'autorisation de créer un connecteur d'action	Écrire	actionconnector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdmin [autorisation uniquement]	Accorde l'autorisation d'approvisionner QuickSight les administrateurs, les auteurs et les lecteurs Amazon	Écrire	user*		
CreateAnalysis	Accorde l'autorisation de créer une analyse à partir d'un modèle.	Écrire	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBrand	Accorde l'autorisation de créer une QuickSight marque Amazon	Écrire	brand*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomPermissions	Accorde l'autorisation de créer une ressource d'autorisations QuickSight personnalisée	Écrire	custompermissions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Accorde l'autorisation de créer un QuickSight tableau de bord	Écrire	dashboard*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Accorde l'autorisation de créer un jeu de données.	Écriture	datasource*		quicksight:PassDataSource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Accorde l'autorisation de créer une source de données.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateEmailCustomizationTemplate [autorisation uniquement]	Accorde l'autorisation de créer un modèle de personnalisation d' QuickSight e-mail	Écrire	emailCustomizationTemplate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtensionAccess [autorisation uniquement]	Accorde l'autorisation de créer un accès à une extension	Écrire	extensionaccess*		
CreateFolder	Accorde l'autorisation de créer un QuickSight dossier	Écrire	folder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	Accorde l'autorisation d'ajouter un QuickSight tableau de bord, une analyse ou un ensemble de données à un QuickSight dossier	Écrire	folder*		
			analysis		
			dashboard		
			dataset		
CreateGroup	Accorde l'autorisation de créer un QuickSight groupe	Écrire	group*		
CreateGroupMembership	Accorde l'autorisation d'ajouter un QuickSight utilisateur à un QuickSight groupe	Écrire	group*	quicksight:UserName	
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIAMPolicyAssignment	Accorde l'autorisation de créer une attribution avec un ARN de politique IAM spécifié qui sera attribuée à des groupes ou utilisateurs spécifiés de QuickSight	Écrire	assignment*		
CreateIngestion	Accorde l'autorisation de démarrer une ingestion SPICE sur un jeu de données.	Écrire	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamespace	Accorde l'autorisation de créer un espace de QuickSight noms	Écrire	namespace*		ds:CreateIdentityPoolDirectory
CreateReader [autorisation uniquement]	Accorde l'autorisation de fournir des QuickSight lecteurs Amazon	Écrire	user*		
CreateRefreshSchedule	Accorde l'autorisation de créer une planification actualisée d'un jeu de données	Écrire	refreshschedule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRoleMembership	Octroie l'autorisation d'ajouter un membre de groupe à un rôle.	Écrire		quicksight:Group	
CreateTemplate	Accorde l'autorisation de créer un modèle.	Écriture	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateAlias	Accorde l'autorisation de créer un alias de modèle.	Écrire	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTheme	Accorde l'autorisation de créer un thème	Écrire	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	Accorde l'autorisation de créer un alias pour une version de thème.	Écrire	theme*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopic	Accorde l'autorisation de créer une rubrique	Écrire	dataset*		quicksight:PassDataSet
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRefreshSchedule	Accorde l'autorisation de créer une planification d'actualisation pour une rubrique	Écrire	topic*		
CreateUser [autorisation uniquement]	Accorde l'autorisation de fournir aux QuickSight auteurs et aux lecteurs Amazon	Écrire	user*		
CreateVPCConnection	Accorde l'autorisation de créer une connexion VPC	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccountCustomPermission	Accorde l'autorisation de supprimer l'autorisation personnalisée associée à un compte	Écrire			
DeleteAccountCustomization	Autorise la suppression d'un compte (personnalisation du QuickSight compte ou de l'espace de noms)	Écrire	customization*		
DeleteAccountSubscription	Accorde l'autorisation de supprimer un QuickSight compte	Écrire	account*		
DeleteActionConnector	Accorde l'autorisation de supprimer un connecteur d'action	Écrire	actionconnector*		
DeleteAnalysis	Accorde l'autorisation de supprimer une analyse.	Écrire	analysis*		
DeleteBrand	Autorise la suppression d'une QuickSight marque Amazon	Écrire	brand*		
DeleteBrandAssignment	Autorise la suppression d'une attribution de marque	Écrire			
DeleteCustomPermissions	Accorde l'autorisation de supprimer une ressource d'autorisations QuickSight personnalisée	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDashboard	Accorde l'autorisation de supprimer un QuickSight tableau de bord	Écrire	dashboard*		
DeleteDataSet	Accorde l'autorisation de supprimer un jeu de données.	Écrire	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataSetRefreshProperties	Accorde l'autorisation de supprimer des propriétés d'actualisation d'un jeu de données	Écrire	dataset*		
DeleteDataSource	Accorde l'autorisation de supprimer une source de données.	Écrire	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDefaultQBusinessApplication	Accorde l'autorisation de supprimer QBusiness l'application associée au QuickSight compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEmailCustomizationTemplate [autorisation uniquement]	Autorise la suppression d'un modèle de personnalisation d' QuickSight e-mail	Écrire	emailCustomizationTemplate*		
DeleteExtensionAccess [autorisation uniquement]	Accorde l'autorisation de supprimer l'accès à une extension	Écrire	extensionaccess*		
DeleteFolder	Accorde l'autorisation de supprimer un QuickSight dossier	Écrire	folder*		
DeleteFolderMembership	Accorde l'autorisation de supprimer un QuickSight tableau de bord, une analyse ou un ensemble de données d'un QuickSight dossier	Écrire	folder*		
			analysis		
			dashboard		
			dataset		
DeleteGroup	Accorde l'autorisation de supprimer un groupe d'utilisateurs de QuickSight	Écrire	group*		
DeleteGroupMembership	Accorde l'autorisation de supprimer un utilisateur d'un groupe afin qu'il ne he/she soit plus membre du groupe	Écrire	group*	quicksight:UserName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteIAMPolicyAssignment	Accorde l'autorisation de mettre à jour une affectation existante.	Écrire	assignment*		
DeleteIdentityPropagationConfig	Accorde l'autorisation de supprimer AWS des services pour une propagation d'identité fiable dans QuickSight	Écrire			
DeleteNamespace	Accorde l'autorisation de supprimer un espace de QuickSight noms	Écrire	namespace*		ds:DeleteDirectory
DeleteRefreshSchedule	Accorde l'autorisation de supprimer une planification actualisée d'un jeu de données	Écrire	refreshschedule*		
DeleteRoleCustomPermission	Octroie l'autorisation de supprimer l'autorisation personnalisée associée à un rôle.	Écrire			
DeleteRoleMembership	Octroie l'autorisation de supprimer un membre du groupe d'un rôle.	Écrire		quicksight:Group	
DeleteTemplate	Accorde l'autorisation de supprimer un modèle.	Écriture	template*		
DeleteTemplateAlias	Accorde l'autorisation de supprimer un alias de modèle.	Écriture	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTheme	Accorde l'autorisation de supprimer un thème.	Écriture	theme*		
DeleteThemeAlias	Accorde l'autorisation de supprimer l'alias d'un thème.	Écrire	theme*		
DeleteTopic	Accorde l'autorisation de supprimer une rubrique	Écrire	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTopicRefreshSchedule	Accorde l'autorisation de supprimer une planification d'actualisation pour une rubrique	Écrire	topic*		
DeleteUser	Accorde l'autorisation de supprimer un QuickSight utilisateur, en fonction de son nom d'utilisateur	Écrire	user*		
DeleteUserByPrincipalId	Accorde l'autorisation de supprimer un utilisateur identifié par son identifiant principal	Écrire	user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteUserCustomPermission	Accorde l'autorisation de supprimer l'autorisation personnalisée associée à un utilisateur	Écrire	user*		
DeleteVPCConnection	Accorde l'autorisation de supprimer une connexion VPC	Écrire	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAccountCustomPermission	Accorde l'autorisation de décrire l'autorisation personnalisée associée à un compte	Lecture			
DescribeAccountCustomization	Accorde l'autorisation de décrire la personnalisation d'un compte pour un QuickSight compte ou un espace de noms	Lecture	customization*		
DescribeAccountSettings	Accorde l'autorisation de décrire les paramètres administratifs du QuickSight compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAccountSubscription	Accorde l'autorisation de décrire un QuickSight compte	Lecture	account*		
DescribeActionConnector	Accorde l'autorisation de décrire un connecteur d'action	Lecture	actionconnector*		
DescribeActionConnectorPermissions	Accorde l'autorisation de décrire les autorisations pour un connecteur d'action	Lecture	actionconnector*		
DescribeAgent [autorisation uniquement]	Accorde l'autorisation de décrire un agent	Lecture	agent*		
DescribeAgentPermissions [autorisation uniquement]	Accorde l'autorisation de décrire les autorisations de l'agent	Lecture	agent*		
DescribeAnalysis	Accorde l'autorisation de décrire une analyse.	Lecture	analysis*		
DescribeAnalysisPermissions	Accorde l'autorisation de décrire des autorisations pour une analyse.	Lecture	analysis*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAssetBundleExportJob	Accorde l'autorisation de décrire une tâche d'exportation d'un bundle de ressources.	Lecture	assetBundleExportJob*		
DescribeAssetBundleImportJob	Accorde l'autorisation de décrire une tâche d'importation d'un bundle de ressources.	Lecture	assetBundleImportJob*		
DescribeAutomationJob	Accorde l'autorisation de décrire une tâche d'automatisation	Lecture	automationJob*		
DescribeBrand	Autorise la description d'une marque	Lecture	brand*		
DescribeBrandAssignment	Accorde l'autorisation de décrire une attribution de marque	Lecture			
DescribeBrandPublishedVersion	Autorise la description de la version publiée de la marque	Lecture	brand*		
DescribeChatConfiguration [autorisation uniquement]	Accorde l'autorisation de décrire la configuration du chat	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCustomPermissions	Accorde l'autorisation de décrire une ressource d'autorisations personnalisée dans un QuickSight compte	Lecture	custompermissions*		
DescribeDashboard	Accorde l'autorisation de décrire un QuickSight tableau de bord	Lecture	dashboard*		
DescribeDashboardPermissions	Accorde l'autorisation de décrire les autorisations pour un QuickSight tableau de bord	Lecture	dashboard*		
DescribeDashboardSnapshotJob	Octroie l'autorisation de décrire une tâche d'instantané de tableau de bord.	Lecture	dashboardSnapshotJob*		
DescribeDashboardSnapshotJobResult	Octroie l'autorisation de décrire le résultat d'une tâche d'instantané de tableau de bord.	Lecture	dashboardSnapshotJob*		
DescribeDashboardsQAConfiguration	Accorde l'autorisation de décrire une configuration de tableau de bord	Lecture			
DescribeDataSet	Accorde l'autorisation de décrire un jeu de données.	Lecture	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetPermissions	Accorde l'autorisation de décrire la politique de ressource d'un jeu de données.	Gestion des autorisations	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetRefreshProperties	Accorde l'autorisation de décrire les propriétés d'actualisation d'un jeu de données	Lecture	dataset*		
DescribeDataSource	Accorde l'autorisation de décrire une source de données	Lecture	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDataSourcePermissions	Accorde l'autorisation de décrire la politique de ressource d'une source de données.	Gestion des autorisations	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDefaultQBusinessApplication	Accorde l'autorisation de décrire QBusiness l'identifiant de l'application associée au QuickSight compte	Lecture			
DescribeEmailCustomizationTemplate [autorisation uniquement]	Accorde l'autorisation de décrire un modèle de personnalisation d' QuickSight e-mail	Lecture	emailCustomizationTemplate*		
DescribeExtensionAccess [autorisation uniquement]	Accorde l'autorisation de décrire l'accès à une extension	Lecture	extensionaccess*		
DescribeFolder	Accorde l'autorisation de décrire un QuickSight dossier	Lecture	folder*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFolderPermissions	Accorde l'autorisation de décrire les autorisations pour un QuickSight dossier	Lecture	folder*		
DescribeFolderResolvedPermissions	Accorde l'autorisation de décrire les autorisations résolues pour un QuickSight dossier	Lecture	folder*		
DescribeGroup	Accorde l'autorisation de décrire un QuickSight groupe	Lecture	group*		
DescribeGroupMembership	Accorde l'autorisation de décrire un membre QuickSight du groupe	Lecture	group*	quicksight:UserName	
DescribeIAMPolicyAssignment	Accorde l'autorisation de décrire une affectation existante.	Lecture	assignment*		
DescribeIngestion	Accorde l'autorisation de décrire une ingestion SPICE sur un jeu de données	Lecture	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeIpRestriction	Accorde l'autorisation de décrire les restrictions d'adresse IP pour le QuickSight compte	Lecture			
DescribeKeyRegistration	Accorde l'autorisation de décrire l'enregistrement QuickSight des clés	Lecture			
DescribeNamespace	Accorde l'autorisation de décrire un espace de QuickSight noms	Lecture	namespace*		
DescribeQPersonalizationConfiguration	Accorde l'autorisation de décrire une configuration de personnalisation	Lecture			
DescribeQuickIndexCapacity [autorisation uniquement]	Accorde l'autorisation de décrire la capacité de l'index	Lecture			
DescribeQuickSightQSearchConfiguration	Accorde l'autorisation de décrire la configuration de QuickSight Q Search	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeRefreshSchedule	Accorde l'autorisation de décrire une planification actualisée d'un jeu de données	Lecture	refreshschedule*		
DescribeRoleCustomPermission	Octroie l'autorisation de décrire l'autorisation personnalisée associée à un rôle.	Lecture			
DescribeSelfUpgradeConfiguration	Accorde l'autorisation de décrire la configuration administrative de mise à niveau automatique associée à un compte	Lecture			
DescribeTemplate	Accorde l'autorisation de décrire un modèle.	Lecture	template*		
DescribeTemplateAlias	Accorde l'autorisation de décrire un alias de modèle.	Lecture	template*		
DescribeTemplatePermissions	Accorde l'autorisation de décrire des autorisations pour un modèle.	Lecture	template*		
DescribeTheme	Accorde l'autorisation de décrire un thème.	Lecture	theme*		
DescribeThemeAlias	Accorde l'autorisation de décrire un alias de thème.	Lecture	theme*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeThemePermissions	Accorde l'autorisation de décrire des autorisations pour un thème.	Lecture	theme*		
DescribeTopic	Accorde l'autorisation de décrire une rubrique	Lecture	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicPermissions	Accorde l'autorisation de décrire la politique de ressources d'une rubrique	Gestion des autorisations	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefresh	Accorde l'autorisation de décrire le statut d'actualisation d'une rubrique	Lecture	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTopicRefreshSchedule	Accorde l'autorisation de décrire une planification d'actualisation pour une rubrique	Lecture	topic*		
DescribeUser	Accorde l'autorisation de décrire un QuickSight utilisateur en fonction de son nom d'utilisateur	Lecture	user*		
DescribeVPCConnection	Accorde l'autorisation de décrire une connexion VPC	Lecture	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GenerateEmbedUrlForAnonymousUser	Accorde l'autorisation de générer une URL utilisée pour intégrer un QuickSight tableau de bord ou une rubrique Q à un utilisateur non inscrit auprès de QuickSight	Écrire	namespace*		
			dashboard		
			theme		
			topic		
				quicksight:AllowedEmbeddingDomains	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GenerateEmbedUrlForRegisteredUser	Accorde l'autorisation de générer une URL utilisée pour intégrer un QuickSight tableau de bord pour un utilisateur inscrit auprès de QuickSight	Écrire	user*		
				quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUserWithIdentity	Accorde l'autorisation de générer une URL utilisée pour intégrer une QuickSight expérience à un utilisateur inscrit à l' QuickSight aide d'une session de rôle améliorée par identité	Écrire		quicksight:AllowedEmbeddingDomains	
GetAnonymousUserEmbedUrl [autorisation uniquement]	Accorde l'autorisation d'obtenir une URL utilisée pour intégrer un QuickSight tableau de bord à un utilisateur non inscrit auprès de QuickSight	Lecture			
GetAuthCode [autorisation uniquement]	Accorde l'autorisation d'obtenir un code d'authentification représentant un utilisateur QuickSight	Lecture	user*		
GetCustomPermissionsSummary [autorisation uniquement]	Accorde l'autorisation d'obtenir des informations sur les autorisations personnalisées d'un compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDashboardEmbedUrl	Accorde l'autorisation d'obtenir une URL utilisée pour intégrer un tableau de bord QuickSight	Lecture	dashboard*		
GetFlowMetadata	Accorde l'autorisation d'obtenir les métadonnées d'un flux	Lecture	flow*		
GetFlowPermissions	Accorde l'autorisation d'obtenir des autorisations pour un flux	Lecture	flow*		
GetGroupMapping [autorisation uniquement]	Accorde l'autorisation d'utiliser Amazon QuickSight, dans l'édition Enterprise, pour identifier et afficher les groupes d'annuaires Microsoft Active Directory (Microsoft Active Directory) mappés à des rôles dans Amazon QuickSight	Lecture			
GetIdentityContext	Accorde l'autorisation d'obtenir le contexte d'identité d'un utilisateur	Lecture	user*		
GetSessionEmbedUrl	Accorde l'autorisation d'obtenir une URL pour intégrer l'expérience de QuickSight console	Lecture			
ListActionConnectors	Accorde l'autorisation de répertorier les connecteurs d'action	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAgents [autorisation uniquement]	Accorde l'autorisation de répertorier les agents	List	agent*		
ListAnalyses	Accorde l'autorisation de répertorier toutes les analyses d'un compte.	List	analysis*		
ListAssetBundleExportJobs	Accorde l'autorisation de répertorier toutes les tâches d'exportation de bundles de ressources.	List	assetBundleExportJob*		
ListAssetBundleImportJobs	Accorde l'autorisation de répertorier toutes les tâches d'importation de bundles de ressources.	List	assetBundleImportJob*		
ListBrands	Autorise la mise en vente de toutes les marques sur un QuickSight compte Amazon	List			
ListCustomPermissions	Accorde l'autorisation de répertorier les ressources d'autorisations personnalisées dans le QuickSight compte	List			
ListCustomerManagedKeys [autorisation uniquement]	Accorde l'autorisation de répertorier toutes les clés gérées par le client qui sont enregistrées	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDashboardVersions	Accorde l'autorisation de répertorier toutes les versions d'un QuickSight tableau de bord	List	dashboard*		
ListDashboards	Accorde l'autorisation de répertorier tous les tableaux de bord d'un compte QuickSight	List	dashboard*		
ListDataSets	Accorde l'autorisation de répertorier tous les jeux de données.	Liste		aws:RequestTag/${TagKey} aws:TagKeys	
ListDataSources	Accorde l'autorisation de répertorier toutes les sources de données.	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListExtensionAccesses [autorisation uniquement]	Accorde l'autorisation de répertorier les accès aux extensions	List			
ListFlows	Accorde l'autorisation de répertorier tous les flux d'un QuickSight compte Amazon	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFolderMembers	Accorde l'autorisation de répertorier tous les membres dans un dossier	Lecture	folder*		
ListFolders	Accorde l'autorisation de répertorier tous les dossiers d'un QuickSight compte	List	folder*		
ListFoldersForResource	Accorde l'autorisation de répertorier tous les dossiers dont une QuickSight ressource est membre	List	analysis		
			dashboard		
			dataset		
			datasource		
			topic		
ListGroupMemberships	Accorde l'autorisation de répertorier des utilisateurs membres d'un groupe.	List	group*		
ListGroups	Accorde l'autorisation de répertorier tous les groupes d'utilisateurs dans QuickSight	List	group*		
ListIAMPolicyAssignments	Accorde l'autorisation de répertorier toutes les missions du QuickSight compte Amazon actuel	List	assignment*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIAMPolicyAssignmentsForUser	Accorde l'autorisation de répertorier toutes les affectations attribuées à un utilisateur et les groupes auxquels il appartient.	List	assignment*		
ListIdentityPropagationConfigs	Accorde l'autorisation de répertorier AWS les services activés pour la propagation d'identités fiables dans QuickSight	List			
ListIngestions	Accorde l'autorisation de répertorier toutes les ingestions SPICE sur un jeu de données.	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListKMSKeysForUser [autorisation uniquement]	Accorde l'autorisation de répertorier les clés KMS d'un utilisateur	List			
ListNamespaces	Permet de répertorier tous les espaces de noms d'un compte QuickSight	List			
ListRefreshSchedules	Accorde l'autorisation de répertorier toutes les planifications actualisées d'un jeu de données	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRoleMemberships	Octroie l'autorisation de répertorier les membres d'un rôle.	List			
ListSelfUpgrades	Permet de répertorier toutes les demandes d'auto-mise à niveau en attente associées à un compte	List	user*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une QuickSight ressource	Lecture	actionconnector		
			analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			emailCustomizationTemplate		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			flow		
			folder		
			template		
			theme		
			topic		
			vpcconnection		
ListTemplateAliases	Accorde l'autorisation de répertorier tous les alias pour un modèle.	Liste	template*		
ListTemplateVersions	Accorde l'autorisation de répertorier toutes les versions d'un modèle.	List	template*		
ListTemplates	Accorde l'autorisation de répertorier tous les modèles d'un QuickSight compte	List	template*		
ListThemeAliases	Accorde l'autorisation de répertorier tous les alias d'un thème.	Liste	theme*		
ListThemeVersions	Accorde l'autorisation de répertorier toutes les versions d'un thème.	Liste	theme*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListThemes	Accorde l'autorisation de répertorier tous les thèmes d'un compte.	List	theme*		
ListTopicRefreshSchedules	Accorde l'autorisation de répertorier toutes les planifications d'actualisation d'une rubrique	List			
ListTopicReviewedAnswers	Accorde l'autorisation de répertorier toutes les réponses révisées pour le sujet	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListTopics	Accorde l'autorisation de répertorier toutes les rubriques	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListUserGroups	Accorde l'autorisation de répertorier des groupes dont un utilisateur donné est membre	List	user*		
ListUsers	Accorde l'autorisation de répertorier tous les QuickSight utilisateurs appartenant à ce compte	List	user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListVPCConnections	Accorde l'autorisation de répertorier toutes les connexions VPC	List		aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSet [autorisation uniquement]	Accorde l'autorisation d'utiliser un jeu de données pour un modèle.	Lecture	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSource [autorisation uniquement]	Accorde l'autorisation d'utiliser une source de données pour un jeu de données.	Lecture	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PredictQAResults	Autorise à prédire les résultats de l'assurance qualité	Lecture	dashboard		
			topic		
PutDataSetRefreshProperties	Accorde l'autorisation de mettre des propriétés d'actualisation d'un jeu de données	Écrire	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
QuickSuiteUsageMetrics [autorisation uniquement]	Accorde l'autorisation d'obtenir des statistiques QuickSuite d'utilisation	Lecture			
RegisterCustomerManagedKey [autorisation uniquement]	Accorde l'autorisation d'enregistrer une clé gérée par le client	Écrire			
RegisterUser	Accorde l'autorisation de créer un QuickSight utilisateur dont l'identité est associée à l'IAM identity/role spécifié dans la demande	Écrire	user*	quicksight:IamArn quicksight:SessionName	
RemoveCustomerManagedKey [autorisation uniquement]	Accorde l'autorisation de supprimer une clé gérée par le client	Écrire			
RestoreAnalysis	Accorde l'autorisation de restaurer une analyse supprimée.	Écrire	analysis*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ScopeDownPolicy [autorisation uniquement]	Accorde l'autorisation de gérer les politiques de délimitation des autorisations relatives aux ressources AWS	Écrire			
SearchActionConnectors	Accorde l'autorisation de rechercher des connecteurs d'action	List	actionconnector*		
SearchAgents [autorisation uniquement]	Autorise les agents de recherche	List	agent*		
SearchAnalyses	Accorde l'autorisation de rechercher un sous-ensemble d'analyses.	List	analysis*		
SearchDashboards	Autorise la recherche d'un sous-ensemble de tableaux de bord QuickSight	List	dashboard*		
SearchDataSets	Accorde l'autorisation de rechercher un sous-ensemble de QuickSight DatSets	List	dataset*		
SearchDataSources	Autorise la recherche d'un sous-ensemble de sources de QuickSight données	List	datasource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchDirectoryGroups [autorisation uniquement]	Accorde l'autorisation d'utiliser Amazon QuickSight, dans l'édition Enterprise, pour afficher vos groupes d'annuaires Microsoft Active Directory afin que vous puissiez choisir ceux à associer aux rôles dans Amazon QuickSight	List			
SearchFlows	Accorde l'autorisation de rechercher des flux dans un QuickSight compte Amazon	List			
SearchFolders	Accorde l'autorisation de rechercher un sous-ensemble de dossiers QuickSight	Lecture	folder*		
SearchGroups	Autorise la recherche d'un sous-ensemble de groupes QuickSight	List	group*		
SearchTopics	Accorde l'autorisation de rechercher un sous-ensemble de sujets	List	topic*		
SearchUsers [autorisation uniquement]	Accorde l'autorisation de rechercher les QuickSight utilisateurs appartenant à ce compte	List	user*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetGroupMapping [autorisation uniquement]	Accorde l'autorisation d'utiliser Amazon QuickSight, dans l'édition Enterprise, pour afficher vos groupes d'annuaires Microsoft Active Directory afin que vous puissiez choisir ceux à associer aux rôles dans Amazon QuickSight	Écrire			
StartAssetBundleExportJob	Accorde l'autorisation de lancer une tâche d'exportation d'un bundle de ressources.	Écrire	assetBundleExportJob*		
StartAssetBundleImportJob	Accorde l'autorisation de lancer une tâche d'importation d'un bundle de ressources.	Écrire	assetBundleImportJob*		
StartAutomationJob	Accorde l'autorisation de démarrer une tâche d'automatisation	Écrire	automation*		
StartDashboardSnapshotJob	Octroie l'autorisation de lancer une tâche d'instantané de tableau de bord.	Écrire	dashboardSnapshotJob*		
StartDashboardSnapshotJobSchedule	Accorde l'autorisation de démarrer un calendrier de tâches instantané sur le tableau de bord	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Subscribe [autorisation uniquement]	Accorde l'autorisation de s'abonner à Amazon QuickSight et permet également à l'utilisateur de passer à l'édition Enterprise	Écrire		quicksight:Edition quicksight:DirectoryType	
TagResource	Accorde l'autorisation d'ajouter des balises à une QuickSight ressource	Identification	actionconnector		
			analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			emailCustomizationTemplate		
			flow		
			folder		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
Unpublish Flow [autorisation uniquement]	Accorde l'autorisation de dépublier un flux	Écrire	flow*		
Unsubscribe [autorisation uniquement]	Accorde l'autorisation de se désabonner d'Amazon QuickSight, ce qui supprime définitivement tous les utilisateurs et leurs ressources d'Amazon QuickSight	Écrire			
UntagResource	Accorde l'autorisation de supprimer des balises d'une QuickSight ressource	Identification	actionconnector		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			emailCustomizationTemplate		
			flow		
			folder		
			ingestion		
			template		
			theme		
			topic		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			vpcconnection		
				aws:TagKeys	
UpdateAccountCustomPermission	Accorde l'autorisation de mettre à jour l'autorisation personnalisée associée à un compte	Écrire			
UpdateAccountCustomization	Accorde l'autorisation de mettre à jour la personnalisation d'un compte pour le QuickSight compte ou l'espace de noms	Écrire	customization*		
UpdateAccountSettings	Accorde l'autorisation de mettre à jour les paramètres administratifs du QuickSight compte	Écrire			
UpdateActionConnector	Accorde l'autorisation de mettre à jour un connecteur d'action	Écrire	actionconnector*		
UpdateActionConnectorPermissions	Accorde l'autorisation de mettre à jour les autorisations pour un connecteur d'action	Gestion des autorisations	actionconnector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgentPermissions [autorisation uniquement]	Accorde l'autorisation de mettre à jour les autorisations des agents	Gestion des autorisations	agent*		
UpdateAnalysis	Accorde l'autorisation de mettre à jour une analyse.	Écriture	analysis*		
UpdateAnalysisPermissions	Accorde l'autorisation de mettre à jour des autorisations pour une analyse.	Gestion des autorisations	analysis*		
UpdateApplicationWithTokenExchangeGrant	Autorise la mise à jour de l'application QuickSight IAM Identity Center avec une subvention Token Exchange	Écrire			
UpdateBrand	Autorise la mise à jour d'une marque	Écrire	brand*		
UpdateBrandAssignment	Autorise la mise à jour d'une attribution de marque	Écrire			
UpdateBrandPublishedVersion	Autorise la mise à jour de la version publiée d'une marque	Écrire	brand*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateChatConfiguration [autorisation uniquement]	Accorde l'autorisation de mettre à jour la configuration du chat	Écrire			
UpdateCustomPermissions	Accorde l'autorisation de mettre à jour une ressource d'autorisations QuickSight personnalisée	Écrire	custompermissions*		
UpdateDashboard	Accorde l'autorisation de mettre à jour un QuickSight tableau de bord	Écrire	dashboard*		
UpdateDashboardLinks	Autorise la mise à jour des liens d'un QuickSight tableau de bord	Écrire	dashboard*		
UpdateDashboardPermissions	Accorde l'autorisation de mettre à jour les autorisations pour un QuickSight tableau de bord	Gestion des autorisations	dashboard*		
UpdateDashboardPublishedVersion	Autorise la mise à jour de la version publiée d'un QuickSight tableau de bord	Écrire	dashboard*		
UpdateDashboardsQAConfiguration	Accorde l'autorisation de mettre à jour une configuration des tableaux de bord	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataSet	Accorde l'autorisation de mettre à jour un jeu de données.	Écriture	dataset*		quicksight:PassDataSource
			datasource		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSetPermissions	Accorde l'autorisation de mettre à jour la politique de ressource d'un jeu de données.	Gestion des autorisations	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSource	Accorde l'autorisation de mettre à jour une source de données.	Écriture	datasource*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataSourcePermissions	Accorde l'autorisation de mettre à jour la politique de ressource d'une source de données.	Gestion des autorisations	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDefaultQBusinessApplication	Autorise la mise à jour de QBusiness l'identifiant de l'application associée au QuickSight compte	Écrire			
UpdateEmailCustomizationTemplate [autorisation uniquement]	Autorise la mise à jour d'un modèle de personnalisation d' QuickSight e-mail	Écrire	emailCustomizationTemplate*		
UpdateExtensionAccess [autorisation uniquement]	Accorde l'autorisation de mettre à jour l'accès à une extension	Écrire	extensionaccess*		
UpdateFlowPermissions	Accorde l'autorisation de mettre à jour les autorisations pour un flux	Gestion des autorisations	flow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFolder	Autorise la mise à jour d'un QuickSight dossier	Écrire	folder*		
UpdateFolderPermissions	Accorde l'autorisation de mettre à jour les autorisations pour un QuickSight dossier	Gestion des autorisations	folder*		
UpdateGroup	Accorde l'autorisation de modifier la description du groupe.	Écriture	group*		
UpdateIAMPolicyAssignment	Accorde l'autorisation de mettre à jour une affectation existante.	Écrire	assignment*		
UpdateIdentityPropagationConfig	Accorde l'autorisation d'ajouter et de mettre à jour AWS des services pour la propagation d'identités fiables dans QuickSight	Écrire			
UpdateIpRestriction	Accorde l'autorisation de mettre à jour les restrictions IP pour le QuickSight compte	Écrire			
UpdateKeyRegistration	Autorise la mise à jour de l'enregistrement QuickSight des clés	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePublicSharingSettings	Accorde l'autorisation d'activer ou de désactiver le partage public sur un compte	Écrire			
UpdateQPersonalizationConfiguration	Accorde l'autorisation de mettre à jour une configuration de personnalisation	Écrire			
UpdateQuickIndexCapacity [autorisation uniquement]	Autorise la mise à jour de la capacité de l'index	Écrire			
UpdateQuickSightQSearchConfiguration	Accorde l'autorisation de mettre à jour la configuration de QuickSight Q Search	Écrire			
UpdateRefreshSchedule	Accorde l'autorisation de mettre à jour une planification actualisée d'un jeu de données	Écrire	refreshschedule*		
UpdateResourcePermissions [autorisation uniquement]	Accorde l'autorisation de mettre à jour les autorisations au niveau des ressources dans QuickSight	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRoleCustomPermission	Octroie l'autorisation de mettre à jour l'autorisation personnalisée associée à un rôle.	Écrire			
UpdateSPICECapacityConfiguration	Autorise la mise à jour de la configuration de capacité QuickSight SPICE	Écrire			
UpdateSelfUpgrade	Permet d'agir sur les demandes de mise à niveau automatique en attente associées à un compte	Écrire	user*		
UpdateSelfUpgradeConfiguration	Accorde l'autorisation de mettre à jour la configuration administrative de mise à niveau automatique associée à un compte	Écrire			
UpdateTemplate	Accorde l'autorisation de mettre à jour un modèle.	Écriture	template*		
UpdateTemplateAlias	Accorde l'autorisation de mettre à jour un alias de modèle.	Écriture	template*		
UpdateTemplatePermissions	Accorde l'autorisation de mettre à jour des autorisations pour un modèle.	Gestion des autorisations	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTheme	Accorde l'autorisation de mettre à jour un thème.	Écriture	theme*		
UpdateThemeAlias	Accorde l'autorisation de mettre à jour l'alias d'un thème.	Écriture	theme*		
UpdateThemePermissions	Accorde l'autorisation de mettre à jour des autorisations pour un thème.	Gestion des autorisations	theme*		
UpdateTopic	Accorde l'autorisation de mettre à jour une rubrique	Écrire	topic*		quicksight:PassDataSet
			dataset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicPermissions	Accorde l'autorisation de mettre à jour la politique de ressources d'une rubrique	Gestion des autorisations	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTopicRefreshSchedule	Accorde l'autorisation de mettre à jour une planification d'actualisation pour une rubrique	Écrire	topic*		
UpdateUser	Accorde l'autorisation de mettre à jour un QuickSight utilisateur Amazon	Écrire	user*		
UpdateUserCustomPermission	Accorde l'autorisation de mettre à jour l'autorisation personnalisée associée à un utilisateur	Écrire	user*		
UpdateVPCConnection	Accorde l'autorisation de mettre à jour une connexion VPC	Écrire	vpcconnection*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Types de ressources définis par Amazon QuickSight

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
account	arn:${Partition}:quicksight:${Region}:${Account}:account/${ResourceId}	
user	arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}	
group	arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}	
analysis	arn:${Partition}:quicksight:${Region}:${Account}:analysis/${ResourceId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}	aws:ResourceTag/${TagKey}
template	arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}	aws:ResourceTag/${TagKey}
vpcconnection	arn:${Partition}:quicksight:${Region}:${Account}:vpcConnection/${ResourceId}	aws:ResourceTag/${TagKey}
assetBundleExportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-export-job/${ResourceId}	
assetBundleImportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-import-job/${ResourceId}	
datasource	arn:${Partition}:quicksight:${Region}:${Account}:datasource/${ResourceId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
ingestion	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/ingestion/${ResourceId}	aws:ResourceTag/${TagKey}
refreshschedule	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/refresh-schedule/${ResourceId}	
theme	arn:${Partition}:quicksight:${Region}:${Account}:theme/${ResourceId}	aws:ResourceTag/${TagKey}
assignment	arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}	
customization	arn:${Partition}:quicksight:${Region}:${Account}:customization/${ResourceId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:quicksight:${Region}:${Account}:namespace/${ResourceId}	
folder	arn:${Partition}:quicksight:${Region}:${Account}:folder/${ResourceId}	aws:ResourceTag/${TagKey}
emailCustomizationTemplate	arn:${Partition}:quicksight:${Region}:${Account}:email-customization-template/${ResourceId}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboardSnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
brand	arn:${Partition}:quicksight:${Region}:${Account}:brand/${ResourceId}	aws:ResourceTag/${TagKey}
custompermissions	arn:${Partition}:quicksight:${Region}:${Account}:custompermissions/${ResourceId}	aws:ResourceTag/${TagKey}
actionconnector	arn:${Partition}:quicksight:${Region}:${Account}:action-connector/${ResourceId}	aws:ResourceTag/${TagKey}
agent	arn:${Partition}:quicksight:${Region}:${Account}:agent/${ResourceId}	
extensionaccess	arn:${Partition}:quicksight:${Region}:${Account}:extension-access/${ResourceId}	
flow	arn:${Partition}:quicksight:${Region}:${Account}:flow/${ResourceId}	aws:ResourceTag/${TagKey}
automation	arn:${Partition}:quicksight:${Region}:${Account}:automation-group/${AutomationGroupId}/automation/${ResourceId}	
automationJob	arn:${Partition}:quicksight:${Region}:${Account}:automation-group/${AutomationGroupId}/automation/${AutomationId}/job/${ResourceId}	
automationGroup	arn:${Partition}:quicksight:${Region}:${Account}:automation-group/${ResourceId}	

Clés de condition pour Amazon QuickSight

Amazon QuickSight définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de balise dans la requête.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés de balise.	ArrayOfString
quicksight:AllowedEmbeddingDomains	Filtre l'accès selon les domaines d'intégration autorisés	ArrayOfString
quicksight:DirectoryType	Filtre l'accès en fonction des options de gestion des utilisateurs	String
quicksight:Edition	Filtre l'accès en fonction de l'édition de QuickSight	String
quicksight:Group	Filtre l'accès par QuickSight groupe (ARN)	ARN
quicksight:IamArn	Filtre l'accès en fonction de l'ARN utilisateur ou du rôle IAM.	ARN

Clés de condition	Description	Type
quicksight:KmsKeyArns	Filtre l'accès par clé KMS ARNs	ArrayOfARN
quicksight:SessionName	Filtre l'accès en fonction du nom de session.	Chaîne
quicksight:UserName	Filtre l'accès en fonction du nom d'utilisateur.	Chaîne

Actions, ressources et clés de condition pour l'API de données Amazon RDS

L'API de données Amazon RDS (préfixe de service : `rds-data`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'API de données Amazon RDS
- Types de ressources définis par l'API de données Amazon RDS
- Clés de condition pour l'API de données Amazon RDS

Actions définies par l'API de données Amazon RDS

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchExecuteStatement	Accorde l'autorisation d'exécuter une instruction SQL par lots sur un tableau de données	Écriture	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
BeginTransaction	Accorde l'autorisation de démarrer une transaction SQL	Écrire	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CommitTransaction	Accorde l'autorisation de mettre fin à une transaction SQL démarrée par l'BeginTransaction opération et valide les modifications	Écrire	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteSql	Accorde l'autorisation d'exécuter une ou plusieurs instructions SQL Cette opération est obsolète. Utiliser	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	l' ExecuteStatement opération BatchExecuteStatement or			aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteStatement	Accorde l'autorisation d'exécuter une instruction SQL sur une base de données	Écriture	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
RollbackTransaction	Accorde l'autorisation de restaurer une transaction La restauration d'une transaction annule les changements apportés	Écriture	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	

Types de ressources définis par l'API de données Amazon RDS

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} aws:TagKeys

Clés de condition pour l'API de données Amazon RDS

L'API de données Amazon RDS définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification associées à la ressource	ArrayOfString

Actions, ressources et clés de condition pour l'authentification IAM Amazon RDS

L'authentification IAM Amazon RDS (préfixe de service : `rds-db`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'authentification IAM Amazon RDS
- Types de ressources définis par l'authentification IAM Amazon RDS
- Clés de condition pour l'authentification IAM Amazon RDS

Actions définies par l'authentification IAM Amazon RDS

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
connect	Permet au rôle IAM ou à l'utilisateur de se connecter à la base de données RDS	Gestion des autorisations	db-user*		

Types de ressources définis par l'authentification IAM Amazon RDS

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
db-user	`arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}`	

Clés de condition pour l'authentification IAM Amazon RDS

L'authentification IAM RDS ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour la AWS corbeille

AWS La corbeille (préfixe de service :`rbin`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Recycle Bin
- Types de ressources définis par AWS Recycle Bin
- Clés de condition pour la AWS corbeille

Actions définies par AWS Recycle Bin

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRule	Accorde l'autorisation de créer une règle de conservation de la corbeille	Écrire	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys rbin:Request/ResourceType	
DeleteRule	Accorde l'autorisation de supprimer une règle de conservation de la corbeille	Écrire	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
GetRule	Accorde l'autorisation d'obtenir des informations détaillées sur	Lecture	rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	une règle de conservation de la corbeille			aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
ListRules	Accorde l'autorisation de répertorier les règles de conservation de la corbeille dans la région	Lecture		rbin:Request/ResourceType	
ListTagsForResource	Accorde l'autorisation de répertorier les balises associées à une ressource	Lecture	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
LockRule	Accorde l'autorisation de verrouiller une règle de conservation de la corbeille existante	Écrire	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter ou de mettre à jour des balises d'une ressource	Identification	rule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UnlockRule	Accorde l'autorisation de déverrouiller une règle de conservation de la corbeille existante	Écrire	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
UntagResource	Accorde l'autorisation de supprimer les balises associées à une ressource.	Identification	rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UpdateRule	Accorde l'autorisation de mettre à jour une règle de conservation de la corbeille existante	Écrire	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Types de ressources définis par AWS Recycle Bin

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
rule	`arn:${Partition}:rbin:${Region}:${Account}:rule/${ResourceName}`	aws:ResourceTag/${TagKey}

Clés de condition pour la AWS corbeille

AWS La corbeille définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString
rbin:Attribute/ResourceType	Filtre l'accès par le type de ressource de la règle existante	String
rbin:Request/ResourceType	Filtre l'accès par le type de ressource dans une demande	String

Actions, ressources et clés de condition pour Amazon Redshift

Amazon Redshift (préfixe de service : `redshift`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Redshift
- Types de ressources définis par Amazon Redshift
- Clés de condition pour Amazon Redshift

Actions définies par Amazon Redshift

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptReservedNodeExchange	Accorde l'autorisation d'échanger un nœud DC1 DC2 réservé contre un nœud réservé sans modification de la configuration	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddPartner	Accorde l'autorisation d'ajouter une intégration de partenaires à un cluster	Écrire			
AssociateDataShareConsumer	Accorde l'autorisation d'associer un consommateur à un datashare	Écriture	datashare*		
				redshift:ConsumerArn redshift:AllowWrites	
AuthorizeClusterSecurityGroupIngress	Accorde l'autorisation d'ajouter une règle entrante (entrée) à un groupe de sécurité Amazon Redshift	Écrire	securitygroup*		
			securitygroupingress-ec2securitygroup*		
AuthorizeDataShare	Accorde l'autorisation d'autoriser un consommateur de datashare spécifié à consommer un datashare	Gestion des autorisations	datashare*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				redshift:ConsumerIdentifier redshift:AllowWrites	
AuthorizeEndpointAccess	Accorde l'autorisation d'autoriser les activités liées au point de terminaison pour le point de terminaison d'un VPC géré par RedShift	Gestion des autorisations			
AuthorizeInboundIntegration [autorisation uniquement]	Autorise Amazon Redshift à valider en permanence que l'entrepôt de données cible peut recevoir des données répliquées depuis l'ARN source	Écrire	integration*		
AuthorizeSnapshotAccess	Accorde l'autorisation à la personne spécifiée Compte AWS de restaurer un instantané	Gestion des autorisations	snapshot*		
BatchDeleteClusterSnapshots	Accorde l'autorisation de supprimer des instantanés dans un lot d'une taille maximale de 100	Écriture	snapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchModifyClusterSnapshots	Accorde l'autorisation de modifier les paramètres d'une liste d'instantanés	Écriture	snapshot*		
CancelQuery [autorisation uniquement]	Accorde l'autorisation d'annuler une requête via la console Amazon Redshift	Écriture			
CancelQuerySession [autorisation uniquement]	Accorde l'autorisation de consulter les requêtes dans la console Amazon Redshift	Écriture			
CancelResize	Accorde l'autorisation d'annuler une opération de redimensionnement	Écriture	cluster*		
CopyClusterSnapshot	Accorde l'autorisation de copier un instantané de cluster	Écrire	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAuthenticationProfile	Accorde l'autorisation de créer un profil d'authentification Amazon Redshift	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCluster	Accorde l'autorisation de créer un cluster.	Écriture	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	Accorde l'autorisation de créer un groupe de paramètres Amazon Redshift	Écriture	parametergroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSecurityGroup	Accorde l'autorisation de créer un groupe de sécurité Amazon Redshift	Écriture	securitygroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSnapshot	Accorde l'autorisation de créer un instantané manuel du cluster spécifié	Écriture	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSubnetGroup	Accorde l'autorisation de créer un groupe de sous-réseaux Amazon Redshift	Écriture	subnetgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterUser	Accorde l'autorisation de créer automatiquement l'utilisateur Amazon Redshift spécifié s'il n'existe pas	Gestion des autorisations	dbuser*		
				redshift:DbUser	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCustomDomainAssociation	Octroie l'autorisation de créer un nom de domaine personnalisé pour un cluster.	Écrire	cluster*		acm:DescribeCertificate
CreateEndpointAccess	Accorde l'autorisation de créer un point de terminaison d'un VPC géré par RedShift	Écrire			
CreateEventSubscription	Accorde l'autorisation de créer un abonnement à la notification d'événement Amazon Redshift	Écriture	eventsubscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmClientCertificate	Accorde l'autorisation de créer un certificat client HSM qu'un cluster utilise pour se connecter à un HSM	Écriture	hsmclientcertificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateHsmConfiguration	Accorde l'autorisation de créer une configuration HSM qui contient les informations requises par un cluster pour stocker et utiliser des clés de chiffrement de base de données dans un module de sécurité matériel (HSM, Hardware Security Module).	Écriture	hsmconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInboundIntegration [autorisation uniquement]	Autorise le principal source à créer une intégration entrante pour que les données soient répliquées de la source vers l'entrepôt de données cible	Écrire			
CreateIntegration	Accorde l'autorisation de créer une intégration Amazon Redshift Zero-ETL	Écrire	integration*		kms:CreateGrant kms:DescribeKey

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys redshift:IntegrationSourceArn redshift:IntegrationTargetArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateQev2IdcApplication [autorisation uniquement]	Accorde l'autorisation de créer une application idc qev2	Écrire			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRedshiftIdcApplication	Octroie l'autorisation de créer une application redshift idc.	Écrire			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
CreateSavedQuery [autorisation uniquement]	Accorde l'autorisation de créer des requêtes SQL enregistrées via la console Amazon Redshift	Écriture			
CreateScheduledAction	Accorde l'autorisation de créer une action planifiée Amazon Redshift	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSnapshotCopyGrant	Accorde l'autorisation de créer une copie instantanée, d'octroyer et de chiffrer des instantanés copiés dans une destination Région AWS	Gestion des autorisations	snapshotcopygrant*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotSchedule	Accorde l'autorisation de créer une planification d'instantané	Écriture	snapshotschedule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Accorde l'autorisation d'ajouter une ou plusieurs balises à la ressource spécifiée	Balisage	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			parameter group		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageLimit	Accorde l'autorisation de créer une limite d'utilisation.	Écrire	usagelimit*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeauthorizeDataShare	Accorde l'autorisation de supprimer l'autorisation du consommateur d'unité de partage des données spécifié pour consommer une unité de partage des données	Gestion des autorisations	datashare*		
				redshift:ConsumerIdentifier	
DeleteAuthenticationProfile	Accorde l'autorisation de supprimer un profil d'authentification Amazon Redshift	Écrire			
DeleteCluster	Accorde l'autorisation de supprimer un cluster précédemment provisionné	Écriture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteClusterParameterGroup	Accorde l'autorisation de supprimer un groupe de paramètres Amazon Redshift	Écriture	parametergroup*		
DeleteClusterSecurityGroup	Accorde l'autorisation de supprimer un groupe de sécurité Amazon Redshift	Écriture	securitygroup*		
DeleteClusterSnapshot	Accorde l'autorisation de supprimer un instantané manuel	Écriture	snapshot*		
DeleteClusterSubnetGroup	Accorde l'autorisation de supprimer un groupe de sous-réseaux de cluster	Écrire	subnetgroup*		
DeleteCustomDomainAssociation	Octroie l'autorisation de supprimer un nom de domaine personnalisé pour un cluster.	Écrire	cluster*		
DeleteEndpointAccess	Accorde l'autorisation de supprimer un point de terminaison d'un VPC géré par Redshift	Écrire			
DeleteEventSubscription	Accorde l'autorisation de supprimer un abonnement à la notification d'événement Amazon Redshift	Écriture	eventsubscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteHsmClientCertificate	Accorde l'autorisation de supprimer un certificat client HSM	Écriture	hsmclientcertificate*		
DeleteHsmConfiguration	Accorde l'autorisation de supprimer une configuration Amazon Redshift HSM	Écrire	hsmconfiguration*		
DeleteIntegration	Autorise la suppression d'une intégration Amazon Redshift Zero-ETL	Écrire	integration*		
				aws:ResourceTag/${TagKey}	
DeletePartner	Accorde l'autorisation de supprimer une intégration de partenaires d'un cluster	Écrire			
DeleteQev2IdcApplication [autorisation uniquement]	Accorde l'autorisation de supprimer une application idc qev2	Écrire	qev2idcapplication*		sso:DeleteApplication
DeleteRedshiftIdcApplication	Octroie l'autorisation de supprimer une application redshift idc.	Écrire	redshiftidcapplication*		sso:DeleteApplication

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteResourcePolicy	Accorde l'autorisation de supprimer la stratégie de ressources pour la ressource spécifiée	Gestion des autorisations	namespace*		
DeleteSavedQueries [autorisation uniquement]	Accorde l'autorisation de supprimer des requêtes SQL enregistrées via la console Amazon Redshift	Écriture			
DeleteScheduledAction	Accorde l'autorisation de supprimer une action planifiée Amazon Redshift	Écriture			
DeleteSnapshotCopyGrant	Accorde l'autorisation de supprimer une autorisation de copie d'instantané	Écriture	snapshotcopygrant*		
DeleteSnapshotSchedule	Accorde l'autorisation de supprimer une planification d'instantané	Écriture	snapshotschedule*		
DeleteTags	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Balisage	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			integration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DeleteUsageLimit	Accorde l'autorisation de supprimer une limite d'utilisation.	Écrire	usagelimit*		
DeregisterNamespace	Accorde l'autorisation de désenregistrer l'espace de noms spécifié auprès d'un consommateur	Écrire			
DescribeAccountAttributes	Accorde l'autorisation de décrire les attributs attachés au paramètre spécifié Compte AWS	Lecture			
DescribeAuthenticationProfiles	Accorde l'autorisation de décrire les profils d'authentification Amazon Redshift créés	Lecture			
DescribeAutonomicsDenylist [autorisation uniquement]	Accorde l'autorisation de décrire la liste des ressources qui sont refusées dans les décisions autonomes globales pour un cluster spécifié	Lecture	cluster*		
DescribeClusterDbRevisions	Accorde l'autorisation de décrire les révisions de base de données pour un cluster	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeClusterParameterGroups	Accorde l'autorisation de décrire des groupes de paramètres Amazon Redshift, y compris les groupes de paramètres que vous avez créés et le groupe de paramètres par défaut.	Lecture			
DescribeClusterParameters	Accorde l'autorisation de décrire les paramètres contenus dans un groupe de paramètres Amazon Redshift	Lecture	parametergroup*		
DescribeClusterSecurityGroups	Accorde l'autorisation de décrire des groupes de sécurité Amazon Redshift	Lecture			
DescribeClusterSnapshots	Accorde l'autorisation de décrire un ou plusieurs objets d'instantané, qui contiennent des métadonnées relatives à vos instantanés de cluster	Lecture			
DescribeClusterSubnetGroups	Accorde l'autorisation de décrire un ou plusieurs objets de groupe de sous-réseaux de cluster, qui contiennent des métadonnées sur vos groupes de sous-réseaux de cluster.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeClusterTracks	Accorde l'autorisation de décrire les pistes de maintenance disponibles	Liste			
DescribeClusterVersions	Accorde l'autorisation de décrire les versions de cluster Amazon Redshift disponibles	Lecture			
DescribeClusters	Accorde l'autorisation de décrire les propriétés des clusters alloués	List	cluster		
DescribeCustomDomainAssociations	Octroie l'autorisation de décrire des noms de domaine personnalisés pour un cluster.	List			
DescribeDataShares	Accorde l'autorisation de décrire les datashare créés et consommés par vos clusters	Read			
DescribeDataSharesForConsumer	Accorde l'autorisation de décrire uniquement les datashare consommés par vos clusters	Read			
DescribeDataSharesForProducer	Accorde l'autorisation de décrire uniquement les datashare créés par vos clusters	Read			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDefaultClusterParameters	Accorde l'autorisation de décrire les paramètres d'une famille de groupes de paramètres	Lecture			
DescribeEndpointAccess	Accorde l'autorisation de décrire des points de terminaison d'un VPC gérés par Redshift	Lecture			
DescribeEndpointAuthorization	Accorde l'autorisation d'autoriser la description d'une activité pour un point de terminaison d'un VPC géré par Redshift	List			
DescribeEventCategories	Accorde l'autorisation de décrire des catégories d'événements pour tous les types de source d'événement ou pour un type de source spécifié	Lecture			
DescribeEventSubscriptions	Accorde l'autorisation de décrire les abonnements aux notifications d'événements Amazon Redshift pour le Compte AWS	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEvents	Accorde l'autorisation de décrire les événements associés aux clusters, aux groupes de sécurité, aux instantanés et aux groupes de paramètres des 14 derniers jours.	Liste			
DescribeHsmClientCertificates	Accorde l'autorisation de décrire les certificats client HSM	Lecture			
DescribeHsmConfigurations	Accorde l'autorisation de décrire les configurations Amazon Redshift HSM	Lecture			
DescribeInboundIntegrations	Accorde l'autorisation de répertorier les intégrations entrantes	List		redshift:InboundIntegrationArn	
DescribeIntegrations	Accorde l'autorisation de décrire une intégration Amazon Redshift Zero-ETL	List	integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeLoggingStatus	Accorde l'autorisation de décrire si des informations, telles que des requêtes et des tentatives de connexion, sont enregistrées pour un cluster	Lecture	cluster*		
DescribeNodeConfigurationOptions	Accorde l'autorisation de décrire les propriétés des configurations de nœuds possibles, telles que le type de nœud, le nombre de nœuds et l'utilisation du disque pour le type d'action spécifié	Liste			
DescribeOrderableClusterOptions	Accorde l'autorisation de décrire les options de cluster pouvant être commandés	Lecture			
DescribePartners	Accorde l'autorisation de récupérer des informations sur les intégrations de partenaires définies pour un cluster	Lecture			
DescribeQev2IdcApplications [autorisation uniquement]	Accorde l'autorisation de décrire les applications idc qev2	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeQuery [autorisation uniquement]	Accorde l'autorisation de décrire une requête via la console Amazon Redshift	Lecture			
DescribeRedshiftIdcApplications	Octroie l'autorisation de décrire des applications redshift idc.	List			sso:GetApplicationGrant sso:ListApplicationAccessScopes
DescribeReservedNodeExchangeStatus	Accorde l'autorisation de décrire les informations de l'état de l'échange et les métadonnées associées pour un échange de nœuds réservés. Les états incluent les valeurs en cours et demandées.	Lecture			
DescribeReservedNodeOfferings	Accorde l'autorisation de décrire les offres de nœuds réservés disponibles par Amazon Redshift	Lecture			
DescribeReservedNodes	Accorde l'autorisation de décrire les nœuds réservés	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeResize	Accorde l'autorisation de décrire la dernière opération de redimensionnement d'un cluster	Lecture	cluster*		
DescribeSavedQueries [autorisation uniquement]	Accorde l'autorisation de décrire les requêtes enregistrées via la console Amazon Redshift	Lecture			
DescribeScheduledActions	Accorde l'autorisation de décrire les actions planifiées Amazon Redshift créées	Lecture			
DescribeSnapshotCopyGrants	Accorde l'autorisation de décrire les autorisations de copie instantanée détenues par la personne spécifiée Compte AWS dans la destination Région AWS	Lecture			
DescribeSnapshotSchedules	Accorde l'autorisation de décrire les planifications d'instantanés	Lecture	snapshotschedule*		
DescribeStorage	Accorde l'autorisation de décrire la taille du stockage des sauvegardes au niveau du compte et le stockage provisoire	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTable [autorisation uniquement]	Accorde l'autorisation de décrire une table via la console Amazon Redshift	Lecture			
DescribeTableRestoreStatus	Accorde l'autorisation de décrire l'état d'une ou de plusieurs demandes de restauration de table effectuées à l'aide de l'action d' RestoreTableFromClusterSnapshot API	Lecture			
DescribeTags	Accorde l'autorisation de décrire les balises	Lecture	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
DescribeUsageLimits	Accorde l'autorisation de décrire des limites d'utilisation.	Lecture	usagelimit*		
DisableLogging	Accorde l'autorisation de désactiver les informations de journalisation, telles que les requêtes et les tentatives de connexion, pour un cluster	Écriture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableSnapshotCopy	Accorde l'autorisation de désactiver la copie automatique des instantanés pour un cluster	Écriture	cluster*		
DisassociateDataShareConsumer	Accorde l'autorisation de dissocier un consommateur d'un datashare	Écriture	datashare*		
				redshift:ConsumerArn	
EnableLogging	Accorde l'autorisation d'activer les informations de journalisation, telles que les requêtes et les tentatives de connexion, pour un cluster	Écriture	cluster*		
EnableSnapshotCopy	Accorde l'autorisation d'activer la copie automatique des instantanés pour un cluster	Écriture	cluster*		
ExecuteQuery [autorisation uniquement]	Accorde l'autorisation d'exécuter une requête via la console Amazon Redshift	Écrire			
FailoverPrimaryCompute	Accorde l'autorisation de basculer le calcul primaire d'un cluster Multi-AZ vers un autre AZ	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
FetchResults [autorisation uniquement]	Accorde l'autorisation d'extraire les résultats de la requête via la console Amazon Redshift	Lecture			
GetClusterCredentials	Accorde l'autorisation d'obtenir des informations d'identification temporaires pour accéder à une base de données Amazon Redshift selon le délai spécifié Compte AWS	Écrire	dbuser*		
			dbname		
				redshift:DbName redshift:DbUser redshift:DurationSeconds	
GetClusterCredentialsWithIAM	Accorde l'autorisation d'obtenir des informations d'identification temporaires améliorées pour accéder à une base de données Amazon Redshift selon le délai spécifié Compte AWS	Écrire	dbname		
				redshift:DbName redshift:DurationSeconds	
GetIdentityCenterAuthToken	Autorise les utilisateurs d'Identity Center à obtenir un jeton autorisé pour accéder aux clusters Redshift	Lecture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetReservedNodeExchangeConfigurationOptions	Accorde l'autorisation d'obtenir des options de configuration pour l'échange de nœuds réservés.	Lecture			
GetReservedNodeExchangeOfferings	Accorde l'autorisation d'obtenir un tableau DC2 ReservedNodeOfferings correspondant au type de paiement, à la durée et au prix d'utilisation du nœud DC1 réservé donné	Lecture			
GetResourcePolicy	Accorde l'autorisation d'obtenir la stratégie de ressources pour la ressource spécifiée	Lecture	namespace*		
JoinGroup	Accorde l'autorisation de rejoindre le groupe Amazon Redshift spécifié	Gestion des autorisations	dbgroup*		
ListDatabases [autorisation uniquement]	Accorde l'autorisation de répertorier des bases de données via la console Amazon Redshift	List			
ListRecommendations	Accorde l'autorisation de répertorier les recommandations des conseillers	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSavedQueries [autorisation uniquement]	Accorde l'autorisation de répertorier les requêtes enregistrées via la console Amazon Redshift	Liste			
ListSchemas [autorisation uniquement]	Accorde l'autorisation de répertorier des schémas via la console Amazon Redshift	Liste			
ListTables [autorisation uniquement]	Accorde l'autorisation de répertorier les tables via la console Amazon Redshift	Liste			
ModifyAquaConfiguration	Accorde l'autorisation de modifier la configuration AQUA d'un cluster	Écrire	cluster*		
ModifyAuthenticationProfile	Accorde l'autorisation de modifier un profil d'authentification Amazon Redshift existant	Écrire			
ModifyAutonomicsDenylist [autorisation uniquement]	Accorde l'autorisation d'ajouter ou de supprimer des ressources de la liste de refus globale des systèmes autonomes pour un cluster spécifié	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyCluster	Accorde l'autorisation de modifier les paramètres d'un cluster	Écriture	cluster*		acm:DescribeCertificate kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:GetRandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
ModifyClusterDbRevision	Accorde l'autorisation de modifier la révision de la base de données d'un cluster	Écrire	cluster*		
ModifyClusterIamRoles	Accorde l'autorisation de modifier la liste des rôles AWS Identity and Access Management (IAM) pouvant être utilisés par un cluster pour accéder à d'autres services AWS	Gestion des autorisations	cluster*		
ModifyClusterMaintenance	Accorde l'autorisation de modifier les paramètres de maintenance d'un cluster	Écriture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyClusterParameterGroup	Accorde l'autorisation de modifier les paramètres d'un groupe de paramètres	Écriture	parametergroup*		
ModifyClusterSnapshot	Accorde l'autorisation de modifier les paramètres d'un instantané	Écriture	snapshot*		
ModifyClusterSnapshotSchedule	Accorde l'autorisation de modifier une planification d'instantanés pour un cluster	Écriture	cluster*		
ModifyClusterSubnetGroup	Accorde l'autorisation de modifier un groupe de sous-réseaux de cluster pour inclure la liste spécifiée de sous-réseaux VPC	Écrire	subnetgroup*		
ModifyCustomDomainAssociation	Octroie l'autorisation de modifier un nom de domaine personnalisé pour un cluster.	Écrire	cluster*		acm:DescribeCertificate
ModifyEndpointAccess	Accorde l'autorisation de modifier un point de terminaison d'un VPC géré par Redshift	Écrire			
ModifyEventSubscription	Accorde l'autorisation de modifier un abonnement de notification d'événement Amazon Redshift existant	Écrire	eventsubscription*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyIntegration	Accorde l'autorisation de modifier une intégration Amazon Redshift Zero-ETL	Écrire	integration*		
				aws:ResourceTag/${TagKey}	
ModifyQev2IdcApplication [autorisation uniquement]	Accorde l'autorisation de modifier une application idc qev2	Écrire	qev2idcapplication*		sso:UpdateApplication

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyRedshiftIdcApplication	Octroie l'autorisation de modifier une application redshift idc.	Écrire	redshiftidcapplication*		sso:DeleteApplicationAccessScope sso:DeleteApplicationGrant sso:GetApplicationGrant sso:ListApplicationAccessScopes sso:PutApplicationAccessScope sso:PutApplicationGrant sso:UpdateApplication

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifySavedQuery [autorisation uniquement]	Accorde l'autorisation de modifier une requête enregistrée existante via la console Amazon Redshift	Écriture			
ModifyScheduledAction	Accorde l'autorisation de modifier une action planifiée Amazon Redshift existante	Écrire			
ModifySnapshotCopyRetentionPeriod	Accorde l'autorisation de modifier le nombre de jours pendant lesquels les instantanés sont conservés dans la destination une Région AWS fois qu'ils ont été copiés depuis la source Région AWS	Écrire	cluster*		
ModifySnapshotSchedule	Accorde l'autorisation de modifier une planification d'instantanés	Écriture	snapshotschedule*		
ModifyUsageLimit	Accorde l'autorisation de modifier une limite d'utilisation.	Écriture	usagelimit*		
PauseCluster	Accorde l'autorisation de suspendre un cluster	Écriture	cluster*		
PurchaseReservedNodeOffering	Accorde l'autorisation d'acheter un nœud réservé	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutResourcePolicy	Accorde l'autorisation de mettre à jour la stratégie de ressources pour la ressource spécifiée	Gestion des autorisations	namespace*		
RebootCluster	Accorde l'autorisation de redémarrer un cluster	Écrire	cluster*		
RegisterNamespace	Accorde l'autorisation d'enregistrer l'espace de noms spécifié à un consommateur	Écrire			
RejectDataShare	Accorde l'autorisation de refuser un datashare partagé à partir d'un autre compte	Gestion des autorisations	datashare*		
ResetClusterParameterGroup	Accorde l'autorisation de définir un ou plusieurs paramètres du groupe de paramètres sur leurs valeurs par défaut et définit les valeurs sources des paramètres sur « engine-default ».	Écriture	parametergroup*		
ResizeCluster	Accorde l'autorisation de modifier la taille d'un cluster	Écriture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreFromClusterSnapshot	Accorde l'autorisation de créer un cluster à partir d'un instantané	Écriture	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
			snapshot*		
				aws:TagKeys	
RestoreTableFromClusterSnapshot	Accorde l'autorisation de créer une table à partir d'une table dans un instantané de cluster Amazon Redshift	Écriture	cluster*		
			snapshot*		
ResumeCluster	Accorde l'autorisation de reprendre l'utilisation d'un cluster	Écriture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RevokeClusterSecurityGroupIngress	Accorde l'autorisation de révoquer une règle d'entrée dans un groupe de sécurité Amazon Redshift pour une plage d'adresses IP ou un groupe de sécurité Amazon EC2 précédemment autorisés.	Écrire	securitygroup*		
			securitygroupingress-ec2securitygroup*		
RevokeEndpointAccess	Accorde l'autorisation de révoquer l'accès aux activités liées au point de terminaison pour un point de terminaison d'un VPC géré par Redshift	Gestion des autorisations			
RevokeSnapshotAccess	Accorde l'autorisation de révoquer l'accès à l'élément spécifié Compte AWS pour restaurer un instantané	Gestion des autorisations	snapshot*		
RotateEncryptionKey	Accorde l'autorisation d'effectuer la rotation d'une clé de chiffrement pour un cluster	Écrire	cluster*		
UpdatePartnerStatus	Accorde l'autorisation de mettre à jour le statut d'une intégration de partenaires	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ViewQueriesFromConsole [autorisation uniquement]	Accorde l'autorisation d'afficher les résultats des requêtes via la console Amazon Redshift	Liste			
ViewQueriesInConsole [autorisation uniquement]	Accorde l'autorisation de mettre fin aux requêtes et chargements en cours d'exécution via la console Amazon Redshift	Liste			

Types de ressources définis par Amazon Redshift

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}
datashare	`arn:${Partition}:redshift:${Region}:${Account}:datashare:${ProducerClusterNamespace}/${DataShareName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
dbgroup	arn:${Partition}:redshift:${Region}:${Account}:dbgroup:${ClusterName}/${DbGroup}	
dbname	arn:${Partition}:redshift:${Region}:${Account}:dbname:${ClusterName}/${DbName}	
dbuser	arn:${Partition}:redshift:${Region}:${Account}:dbuser:${ClusterName}/${DbUser}	
eventsubscription	arn:${Partition}:redshift:${Region}:${Account}:eventsubscription:${EventSubscriptionName}	aws:ResourceTag/${TagKey}
hsmclientcertificate	arn:${Partition}:redshift:${Region}:${Account}:hsmclientcertificate:${HSMClientCertificateId}	aws:ResourceTag/${TagKey}
hsmconfiguration	arn:${Partition}:redshift:${Region}:${Account}:hsmconfiguration:${HSMConfigurationId}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:redshift:${Region}:${Account}:integration:${IntegrationIdentifier}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:redshift:${Region}:${Account}:namespace:${ClusterNamespace}	
parametergroup	arn:${Partition}:redshift:${Region}:${Account}:parametergroup:${ParameterGroupName}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroup:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ec2SecurityGroupId}	aws:ResourceTag/${TagKey}
securitygroupingress-cidr	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/cidrip/${IpRange}	aws:ResourceTag/${TagKey}
securitygroupingress-ec2securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ece2SecuritygroupId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:redshift:${Region}:${Account}:snapshot:${ClusterName}/${SnapshotName}	aws:ResourceTag/${TagKey}
snapshotcopygrant	arn:${Partition}:redshift:${Region}:${Account}:snapshotcopygrant:${SnapshotCopyGrantName}	aws:ResourceTag/${TagKey}
snapshotschedule	arn:${Partition}:redshift:${Region}:${Account}:snapshotschedule:${ScheduleIdentifier}	aws:ResourceTag/${TagKey}
subnetgroup	arn:${Partition}:redshift:${Region}:${Account}:subnetgroup:${SubnetGroupName}	aws:ResourceTag/${TagKey}
usagelimit	arn:${Partition}:redshift:${Region}:${Account}:usagelimit:${UsageLimitId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
redshiftidcapplication	`arn:${Partition}:redshift:${Region}:${Account}:redshiftidcapplication:${RedshiftIdcApplicationId}`	
qev2idcapplication	`arn:${Partition}:redshift:${Region}:${Account}:qev2idcapplication:${Qev2IdcApplicationId}`	

Clés de condition pour Amazon Redshift

Amazon Redshift définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès limité par les actions en fonction de l'ensemble des valeurs autorisées pour chacune des étiquettes	String
aws:ResourceTag/${TagKey}	Filtre l'accès limité par les actions en fonction de la valeur-étiquette associée à la ressource	String
aws:TagKeys	Filtre l'accès limité par les actions en fonction de la présence d'étiquettes obligatoires dans la demande	ArrayOfString
redshift:AllowWrites	Filtre l'accès en fonction du paramètre d'entrée allowWrites.	Booléen

Clés de condition	Description	Type
redshift:ConsumerArn	Filtre l'accès par le consommateur de unité de partage des données	ARN
redshift:ConsumerIdentifier	Filtre l'accès par le consommateur de unité de partage des données	String
redshift:DbName	Filtre l'accès en fonction du nom de la base de données	Chaîne
redshift:DbUser	Filtre l'accès en fonction du nom d'utilisateur de la base de données	Chaîne
redshift:DurationSeconds	Filtre l'accès en fonction du nombre de secondes qui s'écoulent jusqu'à ce qu'un ensemble d'informations d'identification temporaires expire	String
redshift:InboundIntegrationArn	Filtre l'accès par l'ARN d'une ressource d'intégration Zero-ETL entrante	ARN
redshift:IntegrationSourceArn	Filtre l'accès par l'ARN d'une source d'intégration zéro ETL	ARN
redshift:IntegrationTargetArn	Filtre l'accès par l'ARN d'une cible d'intégration zéro ETL	ARN

Actions, ressources et clés de condition pour l'API de données Amazon Redshift

L'API de données Amazon Redshift (préfixe de service : `redshift-data`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'API de données Amazon Redshift
- Types de ressources définis par l'API de données Amazon Redshift
- Clés de condition pour l'API de données Amazon Redshift

Actions définies par l'API de données Amazon Redshift

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchExecuteStatement	Accorde l'autorisation d'exécuter plusieurs requêtes sous une seule connexion	Écrire	cluster		
			workgroup		
				redshift-data:session-owner-iam-userid	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				redshift-data:glue-catalog-arn	
CancelStatement	Accorde l'autorisation d'annuler une requête en cours d'exécution	Écriture		redshift-data:statement-owner-iam-userid	
DescribeStatement	Accorde l'autorisation de récupérer des informations détaillées sur l'exécution d'une instruction	Lecture		redshift-data:statement-owner-iam-userid	
DescribeTable	Accorde l'autorisation de récupérer les métadonnées d'une table particulière	Lecture	cluster*		
			workgroup*		
ExecuteStatement	Accorde l'autorisation d'exécuter une requête	Écrire	cluster		
			workgroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				redshift-data:session-owner-iam-userid redshift-data:glue-catalog-arn	
GetStagingBucketLocation	Accorde l'autorisation d'obtenir l'emplacement du compartiment intermédiaire pour un groupe de travail géré donné	Lecture	managed-workgroup*		
GetStatementResult	Accorde l'autorisation de récupérer le résultat d'une requête	Lecture		redshift-data:statement-owner-iam-userid	
ListDatabases	Accorde l'autorisation de répertorier les bases de données d'un cluster spécifique	Lecture	cluster* workgroup* –		
ListSchemas	Accorde l'autorisation de répertorier les schémas d'un cluster spécifique	Lecture	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			workgroup*		
ListStatements	Accorde l'autorisation de répertorier les requêtes d'un principal spécifique	Liste		redshift-data:statement-owner-iam-userid	
ListTables	Accorde l'autorisation de répertorier les tables d'un cluster spécifique	Liste	cluster*		
			workgroup*		

Types de ressources définis par l'API de données Amazon Redshift

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}	aws:ResourceTag/${TagKey}
managed-workgroup	arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupId}	

Clés de condition pour l'API de données Amazon Redshift

L'API de données Amazon Redshift définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
redshift-data:glue-catalog-arn	Filtre l'accès par barre de catalogue de colle	ARN
redshift-data:session-owner-iam-userid	Filtre l'accès par propriétaire de session (iam userid)	String
redshift-data:statement-	Filtre l'accès en fonction du propriétaire de l'instruction iam userid	String

Clés de condition	Description	Type
owner-iam-userid		

Actions, ressources et clés de condition pour Amazon Redshift sans serveur

Amazon Redshift sans serveur (préfixe de service : `redshift-serverless`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Redshift sans serveur
- Types de ressources définis par Amazon Redshift sans serveur
- Clés de condition pour Amazon Redshift sans serveur

Actions définies par Amazon Redshift sans serveur

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ConvertRecoveryPointToSnapshot	Accorde l'autorisation de convertir un point de récupération en instantané	Écrire	recoveryPoint*		
			snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDomainAssociation	Accorde l'autorisation de créer une association de domaine personnalisée dans Amazon Redshift sans serveur	Écrire	workgroup*		acm:DescribeCertificate
CreateEndpointAccess	Accorde l'autorisation de créer un point de terminaison d'un VPC géré par Amazon RedShift sans serveur	Écrire	endpointAccess*		
CreateNamespace	Accorde l'autorisation de créer un espace de noms Amazon Redshift sans serveur	Écrire	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword secretsmanager:RotateSecret secretsmanager:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReservation	Accorde l'autorisation d'acheter une réservation de capacité conformément à une offre de réservation spécifique, pour un nombre spécifié de RPUs	Écrire			
CreateScheduledAction	Octroie l'autorisation de créer une action planifiée pour un espace de noms Amazon Redshift sans serveur spécifié.	Écrire	namespace*		
CreateSnapshot	Accorde l'autorisation de créer un instantané de toutes les bases de données d'un espace de noms	Écrire	namespace*		
			snapshot*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotCopyConfiguration	Octroie l'autorisation de créer une configuration de copie d'instantané pour un espace de noms Amazon Redshift sans serveur spécifié.	Écrire	namespace*		
CreateUsageLimit	Accorde l'autorisation de créer une limite d'utilisation pour un type d'utilisation Amazon Redshift sans serveur spécifié	Écrire			
CreateWorkgroup	Accorde l'autorisation de créer un groupe de travail dans Amazon Redshift sans serveur	Écrire	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomDomainAssociation	Accorde l'autorisation de supprimer une association de domaines personnalisés	Écrire	workgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEndpointAccess	Accorde l'autorisation de supprimer un point de terminaison d'un VPC géré par Amazon Redshift sans serveur	Écrire	endpointAccess*		
DeleteNamespace	Accorde l'autorisation de supprimer un espace de noms depuis Amazon Redshift sans serveur	Écrire	namespace*		kms:DescribeKey kms:RetireGrant secretsmanager:DeleteSecret secretsmanager:DescribeSecret
DeleteResourcePolicy	Accorde l'autorisation de supprimer la stratégie de ressource spécifiée	Écrire			
DeleteScheduledAction	Octroie l'autorisation de supprimer une action planifiée depuis Amazon Redshift sans serveur.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSnapshot	Accorde l'autorisation de supprimer un instantané depuis Amazon Redshift sans serveur	Écrire	snapshot*		
DeleteSnapshotCopyConfiguration	Octroie l'autorisation de supprimer une configuration de copie d'instantané pour un espace de noms Amazon Redshift sans serveur.	Écrire			
DeleteUsageLimit	Accorde l'autorisation de supprimer une limite d'utilisation depuis Amazon Redshift sans serveur	Écrire			
DeleteWorkgroup	Accorde l'autorisation nécessaire pour supprimer un groupe de travail	Écrire	workgroup*		
DescribeOneTimeCredit [autorisation uniquement]	Accorde l'autorisation de voir sur la console Amazon Redshift sans serveur le nombre de crédits d'essai gratuits restants et leur date d'expiration.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCredentials	Accorde l'autorisation d'obtenir un nom d'utilisateur de la base de données et un mot de passe temporaire avec une autorisation temporaire pour se connecter à Amazon Redshift sans serveur	Écrire	workgroup*		
GetCustomDomainAssociation	Accorde l'autorisation d'obtenir des informations sur une association de domaines personnalisés spécifique	Lecture	workgroup*		
GetEndpointAccess	Accorde l'autorisation de créer un point de terminaison d'un VPC géré par Amazon RedShift sans serveur	Lecture	endpointAccess*		
GetIdentityCenterAuthToken	Autorise les utilisateurs d'Identity Center à obtenir un jeton autorisé pour accéder aux groupes de travail Redshift Serverless	Lecture	workgroup*		
GetManagedWorkgroup	Accorde l'autorisation de créer un groupe de travail Amazon Redshift Managed Serverless avec les paramètres de configuration spécifiés	Lecture	managed-workgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetNamespace	Accorde l'autorisation d'obtenir des informations sur un espace de noms dans Amazon Redshift sans serveur	Lecture	namespace*		
GetRecoveryPoint	Accorde l'autorisation d'obtenir des informations sur un point de récupération	Lecture	recoveryPoint*		
GetReservation	Accorde l'autorisation d'obtenir un objet de réservation particulier	Lecture			
GetReservationOffering	Accorde l'autorisation d'obtenir une offre de réservation particulière	Lecture			
GetResourcePolicy	Accorde l'autorisation d'obtenir une stratégie de ressource	Lecture			
GetScheduledAction	Octroie l'autorisation d'obtenir des informations sur une action planifiée spécifique.	Lecture			
GetSnapshot	Accorde l'autorisation d'obtenir des informations sur un instantané spécifique	Lecture	snapshot*		
GetTableRestoreStatus	Accorde l'autorisation d'obtenir le statut de restauration de tableau sur un instantané spécifique	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTrack	Accorde l'autorisation d'obtenir des informations sur un titre dans Amazon Redshift Serverless	Lecture			
GetUsageLimit	Accorde l'autorisation d'obtenir des informations sur une limite d'utilisation dans Amazon Redshift sans serveur	Lecture			
GetWorkgroup	Accorde l'autorisation d'obtenir des informations sur un groupe de travail spécifique	Lecture	workgroup*		
ListAutonomicsDenylist [autorisation uniquement]	Accorde l'autorisation de répertorier les ressources qui sont refusées dans les décisions autonomes globales pour un groupe de travail spécifié	Lecture	workgroup*		
ListCustomDomainAssociations	Accorde l'autorisation de répertorier les associations de domaines personnalisées dans Amazon Redshift sans serveur	List			
ListEndpointAccess	Permet de répertorier des EndpointAccess objets et des informations pertinentes	List	endpointAccess*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListManagedWorkgroups	Accorde l'autorisation de répertorier les groupes de travail gérés dans Amazon Redshift Serverless	List			
ListNamespaces	Accorde l'autorisation de répertorier des espaces de noms dans Amazon Redshift sans serveur	List			
ListRecoveryPoints	Accorde l'autorisation de répertorier un ensemble de points de récupération	List	recoveryPoint*		
ListReservationOfferings	Accorde l'autorisation de répertorier toutes les offres de réservation de capacité disponibles	List			
ListReservations	Accorde l'autorisation de répertorier toutes les réservations	List			
ListScheduledActions	Octroie l'autorisation de répertorier les actions planifiées.	List			
ListSnapshotCopyConfigurations	Permet de répertorier des SnapshotCopyConfiguration objets et des informations pertinentes	List	namespace		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSnapshots	Accorde l'autorisation de répertorier des instantanés	List	snapshot*		
ListTableRestoreStatus	Accorde l'autorisation de répertorier le statut de restauration de tableau	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises affectées à une ressource	List	namespace		
			workgroup		
				aws:ResourceTag/${TagKey}	
ListTracks	Accorde l'autorisation de répertorier les titres disponibles dans Amazon Redshift Serverless	List			
ListUsageLimits	Accorde l'autorisation de répertorier toutes les limites d'utilisation dans Amazon Redshift sans serveur	List			
ListWorkgroups	Accorde l'autorisation de répertorier des groupes de travail dans Amazon Redshift sans serveur	List			
PutResourcePolicy	Accorde l'autorisation de créer ou de mettre à jour une politique de ressource	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreFromRecoveryPoint	Accorde l'autorisation de restaurer les données à partir d'un point de récupération	Écrire	recoveryPoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreFromSnapshot	Accorde l'autorisation de restaurer un espace de noms à partir d'un instantané	Écrire	snapshot*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
RestoreTableFromRecoveryPoint	Octroie l'autorisation de restaurer une table à partir d'un point de récupération.	Écrire	namespace*		
			recoveryPoint*		
RestoreTableFromSnapshot	Accorde l'autorisation de restaurer un tableau à partir d'un instantané	Écrire	namespace*		
			snapshot*		
TagResource	Accorde l'autorisation d'attribuer une ou plusieurs balises à une ressource	Identification	namespace		
			recoveryPoint		
			snapshot		
			workgroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une balise ou un ensemble de balises d'une ressource	Identification	namespace		
			recoveryPoint		
			snapshot		
			workgroup		
				aws:TagKeys	
UpdateAutonomicsDenylist [autorisation uniquement]	Accorde l'autorisation d'ajouter ou de supprimer des ressources de la liste d'interdiction globale des systèmes autonomes pour un groupe de travail spécifié	Écrire	workgroup *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCustomDomainAssociation	Accorde l'autorisation de mettre à jour un certificat associé à un domaine personnalisé	Écrire	workgroup*		acm:DescribeCertificate
UpdateEndpointAccess	Accorde l'autorisation de mettre à jour un point de terminaison d'un VPC géré par Amazon Redshift sans serveur	Écrire	endpointAccess*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNamespace	Accorde l'autorisation de mettre à jour un espace de noms avec les paramètres de configuration spécifiés	Écrire	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
UpdateScheduledAction	Octroie l'autorisation de mettre à jour une action planifiée.	Écrire			
UpdateSnapshot	Accorde l'autorisation de mettre à jour un instantané	Écrire	snapshot*		
UpdateSnapshotCopyConfiguration	Octroie l'autorisation de mettre à jour une configuration de copie d'instantané pour un espace de noms Amazon Redshift sans serveur.	Écrire			
UpdateUsageLimit	Accorde l'autorisation de mettre à jour d'une limite d'utilisation dans Amazon Redshift sans serveur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateWorkgroup	Accorde l'autorisation de mettre à jour un groupe de travail Amazon Redshift sans serveur avec les paramètres de configuration spécifiés	Écrire	workgroup *		

Types de ressources définis par Amazon Redshift sans serveur

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
namespace	`arn:${Partition}:redshift-serverless:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:redshift-serverless:${Region}:${Account}:snapshot/${SnapshotId}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
managed-workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupName}`	
recoveryPoint	`arn:${Partition}:redshift-serverless:${Region}:${Account}:recoverypoint/${RecoveryPointId}`	aws:ResourceTag/${TagKey}
endpointAccess	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managedvpcendpoint/${EndpointAccessId}`	

Clés de condition pour Amazon Redshift sans serveur

Amazon Redshift sans serveur définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Clés de condition	Description	Type
redshift-serverless:endpointAccessId	Filtre l'accès en fonction de l'identifiant d'accès du point de terminaison	String
redshift-serverless:managedWorkgroupName	Filtre l'accès en fonction de l'identifiant du groupe de travail géré	String
redshift-serverless:namespaceId	Filtre l'accès en fonction de l'identifiant de l'espace de noms	String
redshift-serverless:recoveryPointId	Filtre l'accès en fonction de l'identifiant du point de récupération	String
redshift-serverless:snapshotId	Filtre l'accès en fonction de l'identifiant de l'instantané	String
redshift-serverless:tableRestoreRequestId	Filtre l'accès en fonction de l'identifiant de la requête de restauration du tableau	String
redshift-serverless:workgroupId	Filtre l'accès en fonction de l'identifiant du groupe de travail	String

Actions, ressources et clés de condition pour Amazon Rekognition

Amazon Rekognition (préfixe de service : `rekognition`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Rekognition
- Types de ressources définis par Amazon Rekognition
- Clés de condition pour Amazon Rekognition

Actions définies par Amazon Rekognition

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateFaces	Accorde l'autorisation d'associer plusieurs visages à un même utilisateur	Écrire	collection*		
CompareFaces	Accorde l'autorisation de comparer les visages de	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	l'image d'entrée source à chaque visage détecté dans l'image d'entrée cible				
CopyProjectVersion	Accorde l'autorisation de copier une version de modèle existante vers une nouvelle version de modèle	Écrire	project*		
			projectversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCollection	Accorde l'autorisation de créer une collection dans un Région AWS	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Accorde l'autorisation de créer un jeu de données Amazon Rekognition Custom Labels	Écrire	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateFaceLivenessSession	Accorde l'autorisation de créer une session de détection du visage	Écrire			
CreateProject	Accorde l'autorisation de créer un projet Amazon Rekognition Custom Labels	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProjectVersion	Accorde l'autorisation de commencer la formation d'une nouvelle version d'un modèle	Écrire	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamProcessor	Accorde l'autorisation de créer un processeur de flux Amazon Rekognition	Écrire	collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUser	Accorde l'autorisation de créer un nouvel utilisateur dans une collection à l'aide de l'ID utilisateur unique fourni	Écrire	collection*		
DeleteCollection	Accorde l'autorisation de supprimer la collection spécifiée	Écrire	collection*		
DeleteDataset	Accorde l'autorisation de supprimer un jeu de données Amazon Rekognition Custom Labels existant	Écrire	dataset*		
DeleteFaces	Accorde l'autorisation de supprimer des visages d'une collection	Écrire	collection*		
DeleteProject	Accorde l'autorisation de supprimer un projet	Écrire	project*		
DeleteProjectPolicy	Accorde l'autorisation de supprimer la politique de ressource attachée à un secret	Écrire	project*		
DeleteProjectVersion	Accorde l'autorisation de supprimer un modèle	Écrire	projectversion*		
DeleteStreamProcessor	Accorde l'autorisation de supprimer le processeur de flux spécifié	Écrire	streamprocessor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteUser	Accorde l'autorisation de supprimer un utilisateur d'une collection en fonction de l'ID utilisateur	Écrire	collection*		
DescribeCollection	Accorde l'autorisation de lire les informations d'une collection	Lecture	collection*		
DescribeDataset	Accorde l'autorisation de décrire un jeu de données Amazon Rekognition Custom Labels	Lecture	dataset*		
DescribeProjectVersions	Accorde l'autorisation de répertorier les versions d'un modèle dans un projet Amazon Rekognition Custom Labels	Lecture	project*		
DescribeProjects	Accorde l'autorisation de répertorier les projets Amazon Rekognition Custom Labels	Lecture			
DescribeStreamProcessor	Accorde l'autorisation d'obtenir des informations sur le processeur de flux spécifié	Lecture	streamprocessor*		
DetectCustomLabels	Accorde l'autorisation de détecter des étiquettes personnalisées dans une image fournie	Lecture	projectversion*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DetectFaces	Accorde l'autorisation de détecter des visages humains au sein d'une image fournie comme entrée	Lecture			
DetectLabels	Accorde l'autorisation de détecter les instances d'étiquettes réelles au sein d'une image fournie comme entrée	Lecture			
DetectModerationLabels	Accorde l'autorisation de détecter les étiquettes de modération au sein de l'image d'entrée	Lecture	projectversion		
DetectProtectiveEquipment	Accorde l'autorisation de détecter l'équipement de protection individuelle dans l'image d'entrée	Lecture			
DetectText	Accorde l'autorisation de détecter du texte dans l'image d'entrée et de le convertir en texte lisible par une machine	Lecture			
DisassociateFaces	Accorde l'autorisation de supprimer l'association entre une ID utilisateur et une ID de visage	Écrire	collection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DistributeDatasetEntries	Accorde l'autorisation de distribuer les entrées d'un jeu de données de formation dans le jeu de données de formation et le jeu de données de test d'un projet	Écrire	dataset*		
GetCelebrityInfo	Accorde l'autorisation de lire le nom et les informations supplémentaires d'une célébrité	Lecture			
GetCelebrityRecognition	Accorde l'autorisation de lire les résultats de reconnaissance des célébrités trouvés dans une vidéo stockée par une tâche de reconnaissance asynchrone de célébrités	Lecture			
GetContentModeration	Accorde l'autorisation de lire les résultats de l'analyse de modération de contenu trouvés dans une vidéo stockée par une tâche de modération de contenu asynchrone	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFaceDetection	Accorde l'autorisation de lire les résultats de la détection de visages trouvés dans une vidéo stockée par une tâche de détection de visages asynchrone	Lecture			
GetFaceLivenessSessionResults	Accorde l'autorisation d'obtenir les résultats d'une session de détection du visage	Lecture			
GetFaceSearch	Accorde l'autorisation de lire les visages de la collection correspondants trouvés dans une vidéo stockée par une tâche de recherche de visages asynchrone	Lecture			
GetLabelDetection	Accorde l'autorisation de lire les résultats détectés de l'étiquette trouvés dans une vidéo stockée par une tâche de détection d'étiquettes asynchrone	Lecture			
GetMediaAnalysisJob	Accorde l'autorisation de lire la référence aux résultats d'une tâche dans S3 et des informations supplémentaires sur une tâche d'analyse des médias	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPersonTracking	Accorde l'autorisation de lire la liste des personnes détectées dans une vidéo stockée par une tâche de suivi de personnes asynchrone	Lecture			
GetSegmentDetection	Accorde l'autorisation d'obtenir les segments vidéo trouvés dans une vidéo stockée par une tâche de détection de segments asynchrone	Lecture			
GetTextDetection	Accorde l'autorisation d'obtenir le texte trouvé dans une vidéo stockée par une tâche de détection de texte asynchrone	Lecture			
IndexFaces	Accorde l'autorisation de mettre à jour une collection existante avec des visages détectés dans l'image d'entrée	Écrire	collection*		
ListCollections	Accorde l'autorisation de lire les identifiants de collection dans votre compte	Lecture			
ListDatasetEntries	Accorde l'autorisation de répertorier les entrées du jeu de données dans un jeu de données Amazon Rekognition Custom Labels existant	Lecture	dataset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDatasetLabels	Accorde l'autorisation de répertorier les étiquettes d'un jeu de données	Lecture	dataset*		
ListFaces	Accorde l'autorisation de lire les métadonnées relatives aux visages de la collection spécifiée	Lecture	collection*		
ListMediaAnalysisJobs	Accorde l'autorisation de lire la liste des tâches d'analyse des médias	Lecture			
ListProjectPolicies	Accorde l'autorisation d'obtenir la politique de ressource attachée à un secret	Lecture	project*		
ListStreamProcessors	Accorde l'autorisation d'obtenir une liste de vos processeurs de flux	List			
ListTagsForResource	Accorde l'autorisation de renvoyer une liste de balises associées à une ressource	Lecture	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListUsers	Accorde l'autorisation de mettre UserIds en vente et UserStatus	Lecture	collection*		
PutProjectPolicy	Accorde l'autorisation d'attacher une politique de ressource à un secret	Écrire	project*		
RecognizeCelebrities	Accorde l'autorisation de détecter des célébrités dans l'image d'entrée	Lecture			
SearchFaces	Accorde l'autorisation de rechercher l'ID de visage fourni dans la collection spécifiée	Lecture	collection*		
SearchFacesByImage	Accorde l'autorisation de rechercher le plus grand visage de l'image d'entrée dans la collection spécifiée	Lecture	collection*		
SearchUsers	Accorde l'autorisation de rechercher l'ID de visage ou l'ID utilisateur fourni dans la collection spécifiée pour faire correspondre l'utilisateur	Lecture	collection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchUsersByImage	Accorde l'autorisation de rechercher le plus grand visage de l'image d'entrée dans la collection spécifiée pour faire correspondre l'utilisateur	Lecture	collection*		
StartCelebrityRecognition	Accorde l'autorisation de démarrer la reconnaissance asynchrone des célébrités dans une vidéo stockée	Écrire			
StartContentModeration	Accorde l'autorisation de démarrer la détection asynchrone de contenus explicites ou suggestifs pour adultes dans une vidéo	Écrire			
StartFaceDetection	Accorde l'autorisation de démarrer la détection asynchrone des visages dans une vidéo stockée	Écrire			
StartFaceLivenessSession	Accorde l'autorisation de démarrer la diffusion de vidéos pour une session de détection du visage	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartFaceSearch	Accorde l'autorisation de démarrer la recherche asynchrone de visages d'une collection qui correspondent à ceux des personnes détectées dans une vidéo	Écrire	collection*		
StartLabelDetection	Accorde l'autorisation de démarrer la détection asynchrone des étiquettes dans une vidéo stockée	Écrire			
StartMediaAnalysisJob	Accorde l'autorisation de commencer une tâche d'analyse des médias	Écrire	projectversion		
StartPersonTracking	Accorde l'autorisation de démarrer le suivi asynchrone des personnes dans une vidéo stockée	Écrire			
StartProjectVersion	Accorde l'autorisation de lancer une version de modèle	Écrire	projectversion*		
StartSegmentDetection	Accorde l'autorisation de démarrer la détection asynchrone des segments dans une vidéo stockée	Écrire			
StartStreamProcessor	Accorde l'autorisation de lancer un processeur de flux	Écrire	streamprocessor*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartTextDetection	Accorde l'autorisation de démarrer la détection asynchrone de texte dans une vidéo stockée	Écrire			
StopProjectVersion	Accorde l'autorisation d'arrêter une version de modèle en cours d'exécution	Écrire	projectversion*		
StopStreamProcessor	Accorde l'autorisation d'arrêter un processeur de flux en cours d'exécution	Écrire	streamprocessor*		
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une ressource	Balisage	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource		Identification	collection		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource		dataset		
			project		
			projectversion		
			streamprocessor		
				aws:TagKeys	
UpdateDatasetEntries	Accorde l'autorisation d'ajouter ou de mettre à jour une ou plusieurs lignes JSON (entrées) dans un jeu de données	Écrire	dataset*		
UpdateStreamProcessor	Accorde l'autorisation de modifier les propriétés d'un processeur de flux	Écrire	streamprocessor*		

Types de ressources définis par Amazon Rekognition

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
collection	arn:${Partition}:rekognition:${Region}:${Account}:collection/${CollectionId}	aws:ResourceTag/${TagKey}
streamprocessor	arn:${Partition}:rekognition:${Region}:${Account}:streamprocessor/${StreamprocessorId}	aws:ResourceTag/${TagKey}
project	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/${CreationTimestamp}	aws:ResourceTag/${TagKey}
projectversion	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/version/${VersionName}/${CreationTimestamp}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/dataset/${DatasetType}/${CreationTimestamp}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Rekognition

Amazon Rekognition définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS RePost Private

AWS RePost Private (préfixe de service `:repostspace`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS RePost Private
- Types de ressources définis par AWS RePost Private
- Clés de condition pour AWS RePost Private

Actions définies par AWS RePost Private

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchAddChannelRoleToAccessors	Accorde l'autorisation d'ajouter un rôle aux utilisateurs et aux groupes dans une chaîne privée Re:Post de votre compte	Écrire	space*		
BatchAddRole	Accorde l'autorisation d'ajouter un rôle aux utilisateurs et aux groupes dans un Re:Post privé sur votre compte	Écrire	space*		
BatchRemoveChannelRoleFromAccessors	Autorise les utilisateurs et les groupes à supprimer un rôle dans une chaîne privée Re:Post de votre compte	Écrire	space*		
BatchRemoveRole	Accorde l'autorisation de supprimer un rôle aux utilisateurs et aux groupes dans un Re:Post privé sur votre compte	Écrire	space*		
CreateChannel	Autorise la création d'une nouvelle chaîne en privé Re:post sur votre compte	Écrire	space*		
CreateSpace	Octroie l'autorisation de créer un re:Post privé sur votre compte.	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSpace	Octroie l'autorisation de supprimer un re:Post privé de votre compte.	Écrire	space*		
DeregisterAdmin	Octroie l'autorisation de supprimer un administrateur d'un re:Post privé de votre compte.	Écrire	space*		
GetChannel	Permet d'obtenir la description d'une chaîne en privé Re:post sur votre compte	Lecture	space*		
GetSpace	Octroie l'autorisation d'obtenir la description d'un re:Post privé sur votre compte.	Lecture	space*		
ListChannels	Permet de répertorier toutes les chaînes dans un Re:post privé sur votre compte	Lecture	space*		
ListSpaces	Octroie l'autorisation de répertorier tous les re:Posts privés sur votre compte.	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises associées à une ressource	Lecture	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterAdmin	Accorde l'autorisation d'ajouter un administrateur à un Re:post privé sur votre compte	Écrire	space*		
SendInvites	Octroie l'autorisation d'envoyer des invitations aux utilisateurs d'un re:Post privé sur votre compte.	Écrire	space*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	space*		
				aws:TagKeys	
UpdateChannel	Autorise la mise à jour d'une chaîne en privé Re:post sur votre compte	Écrire	space*		
UpdateSpace	Octroie l'autorisation de mettre à jour un re:Post privé sur votre compte.	Écrire	space*		

Types de ressources définis par AWS RePost Private

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
space	`arn:${Partition}:repostspace:${Region}:${Account}:space/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS RePost Private

AWS RePost Private définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Resilience Hub

AWS Resilience Hub (préfixe de service :`resiliencehub`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Resilience Hub
- Types de ressources définis par AWS Resilience Hub
- Clés de condition pour AWS Resilience Hub

Actions définies par AWS Resilience Hub

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptResourceGroupingRecommendations	Accorde l'autorisation d'accepter les recommandations de regroupement de ressources	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddDraftAppVersionResourceMappings	Accorde l'autorisation d'ajouter des mappages de ressources des projets de version d'application	Écrire	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdateRecommendationStatus	Octroie l'autorisation d'inclure ou d'exclure une ou plusieurs recommandations opérationnelles.	Écrire	application*		
CreateApp	Accorde l'autorisation de créer une application	Écrire	application*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppVersionAppComponent	Accorde l'autorisation de répertorier les composants d'une application	Écrire	application*		
CreateAppVersionResource	Accorde l'autorisation de créer une application	Écrire	application*		
CreateRecommendationTemplate	Accorde l'autorisation de créer un modèle de recommandation	Écrire	application*		s3:CreateBucket s3:ListBucket s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResiliencyPolicy	Accorde l'autorisation de créer une politique de résilience	Écrire	resiliency-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApp	Accorde l'autorisation de supprimer par lots une application	Écrire	application*		
DeleteAppAssessment	Accorde l'autorisation de supprimer par lots l'évaluation des applications	Écrire	application*		
DeleteAppInputSource	Accorde l'autorisation de supprimer la Politique d'une ressource.	Écrire	application*		
DeleteAppVersionAppComponent	Accorde l'autorisation de supprimer un composant	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAppVersionResource	Accorde l'autorisation de répertorier les ressources d'application	Écrire	application*		
DeleteRecommendationTemplate	Accorde l'autorisation de supprimer par lots un modèle de recommandation	Écrire	application*		
DeleteResiliencyPolicy	Accorde l'autorisation de supprimer par lots une politique de résilience	Écrire	resiliency-policy*		
DescribeApp	Accorde l'autorisation de décrire une application	Lecture	application*		
DescribeAppAssessment	Accorde l'autorisation de décrire une évaluation d'application	Lecture	application*		
DescribeAppVersion	Accorde l'autorisation de décrire un modèle de version d'application	Lecture	application*		
DescribeAppVersionAppComponent	Accorde l'autorisation de décrire la version d'une application	Lecture	application*		
DescribeAppVersionResource	Accorde l'autorisation de décrire une résolution d'application	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAppVersionResourcesResolutionStatus	Accorde l'autorisation de décrire une résolution d'application	Lecture	application*		
DescribeAppVersionTemplate	Accorde l'autorisation de décrire un modèle de version d'application	Lecture	application*		
DescribeDraftAppVersionResourcesImportStatus	Accorde l'autorisation de décrire le statut d'importation des ressources des projets de version d'application	Lecture	application*		
DescribeMetricsExport	Accorde l'autorisation de décrire l'exportation des métriques	Lecture			
DescribeResiliencyPolicy	Accorde l'autorisation de décrire une politique de résilience	Lecture	resiliency-policy*		
DescribeResourceGroupingRecommendationTask	Accorde l'autorisation de décrire le dernier statut du processus de recommandation de regroupement	Lecture	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportResourcesToDraftAppVersion	Accorde l'autorisation d'importer des ressources vers le projet de version d'application	Écrire	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAlarmRecommendations	Accorde l'autorisation de répertorier les recommandations d'alarme	List	application*		
ListAppAssessmentComplianceDrifts	Octroie l'autorisation de répertorier les dérives de conformité détectées lors de l'exécution d'une évaluation.	List	application*		
ListAppAssessmentResourceDrifts	Accorde l'autorisation de répertorier les dérives de ressources détectées lors de l'exécution d'une évaluation	List	application*		
ListAppAssessments	Accorde l'autorisation de répertorier les évaluations d'application	List			
ListAppComponentCompliances	Accorde l'autorisation de répertorier les conformités des composants de l'application	List	application*		
ListAppComponentRecommendations	Accorde l'autorisation de répertorier les recommandations de composants	List	application*		
ListAppInputSources	Accorde l'autorisation de répertorier les ressources d'application	List	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAppVersionAppComponents	Accorde l'autorisation de répertorier les composants d'une application	List	application*		
ListAppVersionResourceMappings	Accorde l'autorisation de répertorier les mappages de ressources de la version d'application	List	application*		
ListAppVersionResources	Accorde l'autorisation de répertorier les ressources d'application	List	application*		
ListAppVersions	Accorde l'autorisation de répertorier les versions d'application	List	application*		
ListApps	Accorde l'autorisation de répertorier les applications	List			
ListMetrics	Accorde l'autorisation de répertorier les métriques	List			
ListRecommendationTemplates	Accorde l'autorisation de répertorier les modèles de recommandation	List	application*		
ListResiliencyPolicies	Accorde l'autorisation de répertorier les politiques de résilience	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceGroupingRecommendations	Accorde l'autorisation de répertorier les recommandations de regroupement de ressources	List	application*		
ListSopRecommendations	Accorde l'autorisation de répertorier les recommandations SOP	List	application*		
ListSuggestedResiliencyPolicies	Accorde l'autorisation de répertorier les politiques de résilience suggérées	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture			
ListTestRecommendations	Accorde l'autorisation de répertorier les recommandations de test	List	application*		
ListUnsupportedAppVersionResources	Accorde l'autorisation de répertorier les ressources de version d'application non prises en charge	List	application*		
PublishAppVersion	Accorde l'autorisation de publier une version d'application	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDraftAppVersionTemplate	Accorde l'autorisation de placer un modèle de projet de version d'application	Écrire	application*		
RejectResourceGroupingRecommendations	Autorise le rejet des recommandations de regroupement de ressources	Écrire	application*		
RemoveDraftAppVersionResourceMappings	Accorde l'autorisation de supprimer les mappings du projet de version d'application	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResolveAppVersionResources	Accorde l'autorisation de résoudre les ressources de la version d'application	Écrire	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartAppAssessment	Accorde l'autorisation de créer une évaluation d'application	Écrire	application*		cloudformation:DescribeStacks cloudformation:ListStackResources cloudwatch:DescribeAlarms cloudwatch:GetMetricData cloudwatch:GetMetricStatistics cloudwatch:PutMetricData ec2:DescribeRegions

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					fis:GetExperimentTemplate fis:ListExperimentTemplates fis:ListExperiments resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ssm:GetParametersByPath
				aws:RequestTag/${TagKey} aws:TagKeys	
StartMetricsExport	Autorise le lancement de l'exportation des métriques	Écrire			
StartResourceGroupingRecommendationTask	Autorise le lancement du processus de génération de recommandations de regroupement	Écrire	application*		
TagResource	Accorde l'autorisation d'attribuer une balise de ressource.	Identification	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		
				aws:TagKeys	
UpdateApp	Accorde l'autorisation de mettre à jour une application	Écrire	application*		iam:PassRole
UpdateAppVersion	Accorde l'autorisation de mettre à jour une application	Écrire	application*		
UpdateAppVersionAppComponent	Accorde l'autorisation de mettre à jour un composant	Écrire	application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAppVersionResource	Accorde l'autorisation de mettre à jour une application	Écrire	application*		
UpdateResiliencyPolicy	Accorde l'autorisation de mettre à jour une politique de résilience	Écrire	resiliency-policy*		

Types de ressources définis par AWS Resilience Hub

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
resiliency-policy	`arn:${Partition}:resiliencehub:${Region}:${Account}:resiliency-policy/${ResiliencyPolicyId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:resiliencehub:${Region}:${Account}:app/${AppId}`	aws:ResourceTag/${TagKey}
app-assessment	`arn:${Partition}:resiliencehub:${Region}:${Account}:app-assessment/${AppAssessmentId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
recommendation-template	arn:${Partition}:resiliencehub:${Region}:${Account}:recommendation-template/${RecommendationTemplateId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Resilience Hub

AWS Resilience Hub définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) (préfixe de service :`ram`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Resource Access Manager (RAM)
- Types de ressources définis par AWS Resource Access Manager (RAM)
- Clés de condition pour AWS Resource Access Manager (RAM)

Actions définies par AWS Resource Access Manager (RAM)

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptResourceShareInvitation	Accorde l'autorisation d'accepter l'invitation de partage de ressources spécifiée.	Écrire	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateResourceShare	Accorde l'autorisation d'associer le ou les and/or principaux de ressources à un partage de ressources	Écrire	resource-share*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn ram:RetainSharingOnAccountLeaveOrganization	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateResourceSharePermission	Accorde l'autorisation d'associer une autorisation à un partage de ressources	Écrire	customer-managed-permission*		
			permission*		
			resource-share*		
CreatePermission	Octroie l'autorisation de créer une autorisation qui peut être associée à un partage de ressources.	Écrire		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePermissionVersion	Octroie l'autorisation de créer une nouvelle version d'une autorisation qui peut être associée à un partage de ressources.	Écrire	customer-managed-permission *		
				ram:PermissionArn ram:PermissionResourceType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateResourceShare	Accorde l'autorisation de créer un partage de ressources avec le and/or principal (s) de ressource (s) fourni (s)	Écrire		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal ram:AllowsExternalPrincipals ram:RetainSharingOnAccountLeaveOrganization	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePermission	Octroie l'autorisation de supprimer une autorisation spécifiée.	Écrire	customer-managed-permission*		
				aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType	
DeletePermissionVersion	Octroie l'autorisation de supprimer une version spécifiée d'une autorisation.	Écrire	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
DeleteResourceShare	Accorde l'autorisation de supprimer un partage de ressources	Écrire	resource-share*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RetainSharingOnAccountLeaveOrganization	
DisassociateResourceShare	Accorde l'autorisation de dissocier le ou les and/or principaux de ressources d'un partage de ressources	Écrire	resource-share*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn ram:RetainSharingOnAccountLeaveOrganization	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateResourceSharePermission	Accorde l'autorisation de dissocier une autorisation d'un partage de ressources	Écriture	customer-managed-permission*		
			permission*		
			resource-share*		
EnableSharingWithAwsOrganization	Accorde l'autorisation d'accéder à l'organisation d'un client et de créer un rôle SLR dans le compte du client	Gestion des autorisations			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	Accorde l'autorisation d'obtenir le contenu d'une autorisation AWS RAM	Lecture	customer-managed-permission*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			permission*		
				ram:PermissionArn	
GetResourcePolicies	Accorde l'autorisation d'obtenir des stratégies pour les ressources spécifiées que vous possédez et que vous avez partagées	Lecture			
GetResourceShareAssociations	Accorde l'autorisation d'obtenir un ensemble d'associations de partage des ressources à partir d'une liste fournie ou avec un statut spécifié du type indiqué	Lecture			
GetResourceShareInvitations	Accorde l'autorisation d'obtenir des invitations au partage des ressources de la part de l'ARN d'invitation spécifié ou les invitations pour le partage des ressources.	Lecture			
GetResourceShares	Accorde l'autorisation d'obtenir un ensemble de partages de ressources à partir d'une liste fournie ou avec un statut spécifié	Lecture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPendingInvitationResources	Accorde l'autorisation de répertorier les ressources figurant dans un partage de ressources partagé avec vous, mais pour lequel l'invitation est toujours en attente	Lecture	resource-share-invitation*		
				ram:ResourceShareName	
ListPermissionAssociations	Accorde l'autorisation de répertorier des informations sur l'autorisation et toute association	List	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	Accorde l'autorisation de répertorier les versions d'une autorisation AWS RAM	List			
ListPermissions	Accorde l'autorisation de AWS répertorier les autorisations de RAM	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPrincipals	Accorde l'autorisation de répertorier les mandataires avec qui vous avez partagé des ressources ou qui ont partagé des ressources avec vous	List			
ListReplacePermissionAssociationsWork	Octroie l'autorisation de récupérer le statut du remplacement d'autorisation asynchrone.	List			
ListResourceSharePermissions	Accorde l'autorisation de répertorier les autorisations associées à un partage de ressources	List	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RetainSharingOnAccountLeaveOrganization	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceTypes	Accorde l'autorisation de répertorier les types de ressources partageables pris en charge par la RAM AWS	List			
ListResources	Accorde l'autorisation de répertorier les ressources que vous avez ajoutées à des partages de ressources ou les ressources partagées avec vous	List			
ListSourceAssociations	Accorde l'autorisation de répertorier les associations de sources pour les partages de ressources	List			
PromotePermissionCreatedFromPolicy	Octroie l'autorisation de créer une autorisation distincte et entièrement gérable gérée par le client.	Écrire	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PromoteResourceShareCreatedFromPolicy	Accorde l'autorisation de promouvoir le partage de ressources spécifié	Écriture	resource-share*		
RejectResourceShareInvitation	Accorde l'autorisation de refuser l'invitation de partage de ressources spécifiée	Écrire	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
ReplacePermissionAssociations	Accorde l'autorisation de mettre à jour tous les partages de ressources vers une nouvelle autorisation	Écrire	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetDefaultPermissionVersion	Octroie l'autorisation de spécifier un numéro de version comme version par défaut pour l'autorisation gérée par le client correspondante.	Écrire	customer-managed-permission *		
				ram:PermissionArn ram:PermissionResourceType	
TagResource	Octroie l'autorisation de baliser le partage de ressources spécifié ou l'autorisation spécifiée.	Identification	customer-managed-permission		
			resource-share		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Octroie l'autorisation d'annuler le balisage du partage de ressources spécifié ou de l'autorisation spécifiée.	Identification	customer-managed-permission		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			resource-share		
				aws:TagKeys	
UpdateResourceShare	Accorde l'autorisation de mettre à jour des attributs du partage de ressources	Écrire	resource-share*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RequestedAllowsExternalPrincipals ram:RetainSharingOnAccountLeaveOrganization	

Types de ressources définis par AWS Resource Access Manager (RAM)

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
resource-share	`arn:${Partition}:ram:${Region}:${Account}:resource-share/${ResourcePath}`	aws:ResourceTag/${TagKey} ram:AllowsExternalPrincipals ram:ResourceShareName
resource-share-invitation	`arn:${Partition}:ram:${Region}:${Account}:resource-share-invitation/${ResourcePath}`	ram:ShareOwnerAccountId
permission	`arn:${Partition}:ram::${Account}:permission/${ResourcePath}`	ram:PermissionArn ram:PermissionResourceType
customer-managed-permission	`arn:${Partition}:ram:${Region}:${Account}:permission/${ResourcePath}`	aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType

Clés de condition pour AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les accès en fonction des balises qui sont transmises dans la demande lors de la création ou du balisage d'un partage de ressources. Si les utilisateurs ne transmettent pas ces identifications spécifiques ou s'ils ne spécifient pas du tout de identifications, la demande échoue.	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise qui sont transmises lors de la création ou du balisage d'un partage de ressources	ArrayOfString
ram:AllowsExternalPrincipals	Filtre l'accès en fonction des partages de ressources qui autorisent ou refusent le partage avec des principaux externes. Par exemple, spécifiez la valeur true si l'action ne peut être effectuée que sur les partages de ressources qui autorisent le partage avec des mandataires externes. Les principaux externes sont AWS des comptes extérieurs à son organisation AWS	Booléen
ram:PermissionArn	Filtre l'accès en fonction de l'ARN d'autorisation spécifié	ARN
ram:PermissionResourceType	Filtre l'accès en fonction des autorisations du type de ressource spécifié	String
ram:Principal	Filtre l'accès en fonction du format du principal spécifié	String
ram:RequestedAllow	Filtre l'accès en fonction de la valeur spécifiée pour « allowExternalPrincipals ». Les principaux externes sont AWS des comptes extérieurs à son organisation AWS	Booléen

Clés de condition	Description	Type
sExternal Principals		
ram:Reque stedResou rceType	Filtre l'accès en fonction du type de ressource spécifié	String
ram:Resou rceArn	Filtre l'accès en fonction de l'ARN spécifiée	ARN
ram:Resou rceShareName	Filtre l'accès en fonction d'un partage de ressources avec le nom spécifié	String
ram:Resou rceTag/${ TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String
ram:Retai nSharingO nAccountL eaveOrgan ization	Filtre l'accès en RetainSharingOnAccountLeaveOrganizat ion fonction de ResourceShareConfiguration la valeur définie sur le partage des ressources	Booléen
ram:Share OwnerAccountId	Filtre l'accès en fonction des partages de ressources appartenant à un compte spécifique. Par exemple, vous pouvez utiliser cette clé de condition pour spécifier les invitations au partage de ressources qui peuvent être acceptées ou rejetées en fonction de l'ID de compte du propriétaire du partage des ressources	String

Actions, ressources et clés de condition pour AWS Resource Explorer

AWS L'explorateur de ressources (préfixe de service :`resource-explorer-2`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Resource Explorer
- Types de ressources définis par AWS Resource Explorer
- Clés de condition pour AWS Resource Explorer

Actions définies par AWS Resource Explorer

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateDefaultView	Accorde l'autorisation de définir la vue spécifiée comme vue par défaut pour cela Région AWS dans ce Compte AWS	Écrire			
BatchGetView	Accorde l'autorisation de récupérer des détails sur les vues que vous spécifiez par une liste de ARNs	Lecture			resource-explorer-2:GetView

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIndex	Accorde l'autorisation d'activer l'explorateur de ressources Région AWS dans l'opération dans laquelle vous avez appelé cette opération en créant un index	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedView [autorisation uniquement]	Accorde l'autorisation de créer une vue gérée	Écrire			
CreateResourceExplorerSetup	Accorde l'autorisation de créer une configuration d'explorateur de ressources	Écrire			
CreateStreamingAccessForService [autorisation uniquement]	Accorde l'autorisation de créer un accès en streaming à l'explorateur de ressources	Écrire			
CreateView	Accorde l'autorisation de créer une vue que les utilisateurs peuvent interroger	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteIndex	Accorde l'autorisation de désactiver l'explorateur de ressources dans le champ spécifié Région AWS en supprimant l'index	Écrire	index*		
DeleteResourceExplorerSetup	Autorise la suppression de la configuration de l'explorateur de ressources	Écrire			
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer la politique de ressources de la vue spécifiée	Gestion des autorisations	view*		
DeleteStreamingAccessForService [autorisation uniquement]	Autorise la suppression de l'accès au streaming de l'explorateur de ressources	Écrire			
DeleteView	Accorde l'autorisation de supprimer une vue	Écrire	view*		
DisassociateDefaultView	Accorde l'autorisation de supprimer la vue par défaut pour le Région AWS dans lequel vous appelez cette opération	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountLevelServiceConfiguration	Accorde à Resource Explorer l'autorisation d'accéder aux données au niveau du compte au sein de votre AWS organisation	Lecture			
GetDefaultView	Accorde l'autorisation de récupérer le nom de ressource Amazon (ARN) de la vue par défaut pour l'opération Région AWS dans laquelle vous appelez cette opération	Lecture			
GetIndex	Accorde l'autorisation de récupérer des informations sur l'index Région AWS dans lequel vous appelez cette opération	Lecture			
GetManagedView	Accorde l'autorisation d'obtenir une vue gérée	Lecture	managed-view*		
GetResourceExplorerSetup	Accorde l'autorisation de configurer l'explorateur de ressources	Lecture			
GetResourcePolicy [autorisation uniquement]	Accorde l'autorisation de récupérer des informations sur la politique de ressources de la vue spécifiée	Lecture	view*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceIndex	Accorde l'autorisation d'obtenir l'index des services	Lecture			
GetServiceView	Accorde l'autorisation d'accéder à la vue du service	Lecture			
GetView	Accorde l'autorisation de récupérer des informations sur la vue spécifiée	Lecture	view*		
ListIndexes	Accorde l'autorisation de répertorier tous les index Régions AWS	List			
ListIndexesForMembers	Accorde l'autorisation de répertorier les index du compte membre de l'organisation dans tous Régions AWS	List			
ListManagedViews	Accorde l'autorisation de répertorier les vues gérées	List			
ListServiceIndexes	Accorde l'autorisation de répertorier les index des services dans tous Régions AWS	List			
ListServiceViews	Accorde l'autorisation de répertorier les vues des services dans tous Régions AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListStreamingAccessForServices	Accorde l'autorisation de répertorier les accès au streaming pour les services	List			
ListSupportedResourceTypes	Accorde l'autorisation de récupérer une liste de tous les types de ressources actuellement pris en charge par l'Explorateur de ressources	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises qui sont attachées à la ressource spécifiée	Lecture	index view		
ListViews	Accorde l'autorisation de répertorier les noms de ressources Amazon (ARNs) de toutes les vues disponibles Région AWS dans le cadre duquel vous appelez cette opération	List			
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de mettre à jour la politique de ressources de la vue spécifiée	Gestion des autorisations	view*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Search	Accorde l'autorisation de rechercher des ressources et d'afficher les détails de toutes les ressources correspondant aux critères spécifiés	Lecture	view*		
				resource-explorer-2:Operation	
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs paires clé-valeur de balise à la ressource spécifiée	Identification	index		
			view		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs paires clé-valeur de balise de la ressource spécifiée	Identification	index		
			view		
				aws:TagKeys	
UpdateIndexType	Accorde l'autorisation de modifier le type de l'index de LOCAL à AGGREGATOR ou inversement	Écrire	index*		
UpdateView	Accorde l'autorisation de modifier certains détails d'une vue	Écrire	view*		

Types de ressources définis par AWS Resource Explorer

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
view	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${ViewUuid}`	aws:ResourceTag/${TagKey}
index	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${IndexUuid}`	aws:ResourceTag/${TagKey}
managed-view	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:managed-view/${ManagedViewName}/${ManagedViewUuid}`	

Clés de condition pour AWS Resource Explorer

AWS Resource Explorer définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des clés de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
resource-explorer-2:Operation	Filtre l'accès en fonction de l'opération réellement invoquée, des valeurs disponibles : Rechercher, ListResources	String

Actions, ressources et clés de condition pour l'API de balisage des groupes de ressources Amazon

L'API de balisage des groupes de ressources Amazon (préfixe de service : `tag`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'API de balisage des groupes de ressources Amazon
- Types de ressources définis par l'API de balisage des groupes de ressources Amazon
- Clés de condition pour l'API de balisage des groupes de ressources Amazon

Actions définies par l'API de balisage des groupes de ressources Amazon

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReportCreation	Accorde l'autorisation de décrire le statut de l' StartReportCreation opération	Lecture			
GetComplianceSummary	Accorde l'autorisation de récupérer un résumé du nombre de ressources non conformes avec leurs politiques de balisage efficaces	Lecture			
GetResources	Accorde l'autorisation de renvoyer des ressources étiquetées ou précédemment étiquetées dans le champ spécifié Région AWS pour le compte appelant	Lecture			
GetTagKeys	Accorde l'autorisation de renvoyer les clés de balise actuellement utilisées dans le compte spécifié Région AWS pour le compte appelant	Lecture			
GetTagValues	Accorde l'autorisation de renvoyer les valeurs de balise	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	pour la clé spécifiée qui sont utilisées dans la clé spécifiée Région AWS pour le compte appelant				
ListRequiredTags	Accorde l'autorisation de répertorier les balises requises pour les types de ressources pris en charge dans le compte d'appel	List			
StartReportCreation	Accorde l'autorisation de commencer à générer un rapport répertoriant toutes les ressources balisées dans les comptes de votre organisation, et si chaque ressource est conforme à la politique de balise efficace	Écrire			
TagResources	Accorde l'autorisation d'appliquer une ou plusieurs balises aux ressources spécifiées	Identification			
UntagResources	Accorde l'autorisation de supprimer les balises spécifiées des ressources spécifiées	Identification			

Types de ressources définis par l'API de balisage des groupes de ressources Amazon

L'API de balisage des groupes de ressources Amazon ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de stratégie IAM. Pour autoriser l'accès à l'API de balisage des groupes de ressources Amazon, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour l'API de balisage des groupes de ressources Amazon

Le balisage des groupes de ressources ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Resource Groups

AWS Resource Groups (préfixe de service :`resource-groups`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Resource Groups
- Types de ressources définis par AWS Resource Groups
- Clés de condition pour AWS Resource Groups

Actions définies par AWS Resource Groups

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateResource [autorisation uniquement]	Accorde l'autorisation d'associer une ressource à une application	Écrire	group*		
CancelTagSyncTask	Accorde l'autorisation d'annuler une tâche de synchronisation de balises pour un groupe d'applications	Écrire	group*		resource-groups:DeleteGroup
CreateGroup	Accorde l'autorisation de créer un groupe de ressources avec un nom, une description et une requête de ressource spécifiés	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks
DeleteGroup	Accorde l'autorisation de supprimer un groupe de ressources spécifié	Écrire	group*		tag:GetResources
DeleteGroupPolicy [autorisation uniquement]	Accorde l'autorisation de supprimer une politique basée sur les ressources pour le groupe spécifié	Écrire	group*		
DisassociateResource [autorisation uniquement]	Accorde l'autorisation de dissocier une ressource d'une application	Écrire	group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountSettings	Accorde l'autorisation d'obtenir l'état actuel de la configuration de la zone Resource Groups	Lecture			
GetGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de ressources spécifié	Lecture	group*		
GetGroupConfiguration	Accorde l'autorisation d'obtenir la configuration de service associée au groupe de ressources spécifié	Lecture	group*		
GetGroupPolicy [autorisation uniquement]	Accorde l'autorisation d'obtenir une politique basée sur les ressources pour le groupe spécifié	Lecture	group*		
GetGroupQuery	Accorde l'autorisation d'obtenir la requête associée à un groupe de ressources spécifié	Lecture	group*		
GetTagSyncTask	Accorde l'autorisation d'obtenir des informations sur une tâche de synchronisation de balises spécifiée	Lecture	group*		
GetTags	Accorde l'autorisation d'obtenir les balises associées à un groupe de ressources spécifié	Lecture	group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GroupResources	Accorde l'autorisation d'ajouter les ressources spécifiées au groupe spécifié	Écriture	group*		resource-groups:Tag tag:TagResources
ListGroupResources	Accorde l'autorisation de répertorier les ressources membres d'un groupe de ressources spécifié	List	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
ListGroupingStatuses	Accorde l'autorisation de répertorier les statuts de regroupement pour un groupe d'applications spécifié	List	group*		
ListGroups	Accorde l'autorisation de répertorier tous les groupes de ressources de votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceTypes [autorisation uniquement]	Accorde l'autorisation de répertorier les types de ressources pris en charge	List			
ListTagSyncTasks	Accorde l'autorisation de répertorier toutes les tâches de synchronisation de balises de votre compte	List	group*		
PutGroupConfiguration	Accorde l'autorisation d'utiliser la configuration de service associée au groupe de ressources spécifié	Écriture	group*		
PutGroupPolicy [autorisation uniquement]	Accorde l'autorisation d'ajouter une politique basée sur les ressources pour le groupe spécifié	Écrire	group*		
SearchResources	Accorde l'autorisation de rechercher AWS des ressources correspondant à la requête donnée	List			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartTagSyncTask	Accorde l'autorisation de créer une tâche de synchronisation de balises pour un groupe d'applications	Écrire	group*		iam:PassRole resource-groups:CreateGroup
Tag	Accorde l'autorisation de baliser un groupe de ressources spécifié	Balisage	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UngroupResources	Accorde l'autorisation de supprimer les ressources spécifiées du groupe spécifié	Écriture	group*		resource-groups:Untag tag:UntagResources
Untag	Accorde l'autorisation de supprimer les balises associées à un groupe de ressources spécifié	Identification	group*		
				aws:TagKeys	
UpdateAccountSettings	Accorde l'autorisation de mettre à jour des fonctions optionnelles dans des Resource Groups	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGroup	Accorde l'autorisation de mettre à jour un groupe de ressources spécifié	Écriture	group*		
UpdateGroupQuery	Accorde l'autorisation de mettre à jour la requête associée à un groupe de ressources spécifié	Écrire	group*		cloudformation:DescribeStacks

Types de ressources définis par AWS Resource Groups

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
group	`arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}`	aws:ResourceTag/${TagKey}
tagSyncTask	`arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}/tag-sync-task/${TaskId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Resource Groups

AWS Resource Groups définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le portail de la RHEL Knowledgebase Amazon.

Portail de la RHEL Knowledgebase Amazon (préfixe de service : `rhelkb`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes pour leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le portail de la RHEL Knowledgebase Amazon.
- Types de ressources définis par le portail de la RHEL Knowledgebase Amazon.
- Clés de condition pour le portail de la RHEL Knowledgebase Amazon.

Actions définies par le portail de la RHEL Knowledgebase Amazon.

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRhelURL	Accorde l'autorisation d'accéder au portail Red Hat Knowledgebase.	Lecture			

Types de ressources définis par le portail de la RHEL Knowledgebase Amazon.

Le portail de la RHEL Knowledgebase Amazon ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de politique IAM. Pour autoriser l'accès au portail de la RHEL Knowledgebase Amazon, spécifiez `"Resource": "*"` dans la politique.

Clés de condition pour le portail de la RHEL Knowledgebase Amazon.

RHEL KB ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politiques. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS RoboMaker

AWS RoboMaker (préfixe de service :`robomaker`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS RoboMaker
- Types de ressources définis par AWS RoboMaker
- Clés de condition pour AWS RoboMaker

Actions définies par AWS RoboMaker

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDeleteWorlds	Supprime un ou plusieurs environnements dans une opération par lots.	Écriture			
BatchDescribeSimulationJob	Décrit plusieurs tâches de simulation.	Lecture			
CancelDeploymentJob	Annule une tâche de déploiement.	Écriture	deploymentJob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelSimulationJob	Annule une tâche de simulation.	Écriture	simulationJob*		
CancelSimulationJobBatch	Annule un lot de tâches de simulation.	Écriture	simulationJobBatch*		
CancelWorldExportJob	Annule une tâche d'exportation d'environnement.	Écriture	worldExportJob*		
CancelWorldGenerationJob	Annule une tâche de génération d'environnement.	Écriture	worldGenerationJob*		
CreateDeploymentJob	Crée une tâche de déploiement.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateFleet	Crée une flotte de déploiement qui représente un groupe logique de robots exécutant la même application robotique.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRobot	Crée un robot qui peut être enregistré dans une flotte.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateRobotApplication	Crée une application robotique.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobotApplicationVersion	Crée un instantané d'une application robotique.	Écriture	robotApplication*		s3:GetObject
CreateSimulationApplication	Crée une application de simulation.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSimulationApplicationVersion	Crée un instantané d'une application de simulation.	Écriture	simulationApplication*		s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSimulationJob	Crée une tâche de simulation.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateWorldExportJob	Crée une tâche d'exportation d'environnement.	Écriture	world*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldGenerationJob	Crée une tâche de génération d'environnement.	Écriture	worldTemplate*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldTemplate	Crée un modèle d'environnement.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFleet	Supprime une flotte de déploiement.	Écriture	deploymentFleet*		
DeleteRobot	Supprime un robot.	Écriture	robot*		
DeleteRobotApplication	Supprime une application robotique.	Écriture	robotApplication*		
DeleteSimulationApplication	Supprime une application de simulation.	Écriture	simulationApplication*		
DeleteWorldTemplate	Supprime un modèle d'environnement.	Écriture	worldTemplate*		
DeregisterRobot	Annule l'enregistrement d'un robot dans une flotte.	Écriture	deploymentFleet* robot*		
DescribeDeploymentJob	Décrit une tâche de déploiement.	Lecture	deploymentJob*		
DescribeFleet	Décrit une flotte de déploiement.	Lecture	deploymentFleet*		
DescribeRobot	Décrit un robot.	Lecture	robot*		
DescribeRobotApplication	Décrit une application robotique.	Lecture	robotApplication*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSimulationApplication	Décrit une application de simulation.	Lecture	simulationApplication*		
DescribeSimulationJob	Décrit une tâche de simulation.	Lecture	simulationJob*		
DescribeSimulationJobBatch	Décrit un lot de tâches de simulation	Lecture	simulationJobBatch*		
DescribeWorld	Décrit un environnement.	Lecture	world*		
DescribeWorldExportJob	Décrit une tâche d'exportation d'environnement.	Lecture	worldExportJob*		
DescribeWorldGenerationJob	Décrit une tâche de génération d'environnement.	Lecture	worldGenerationJob*		
DescribeWorldTemplate	Décrit un modèle d'environnement.	Lecture	worldTemplate*		
GetWorldTemplateBody	Récupère le corps d'un modèle d'environnement.	Lecture	worldTemplate*		
ListDeploymentJobs	Répertorie les tâches de déploiement.	Liste			
ListFleets	Répertorie les flottes.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRobotApplications	Répertorie les applications robotiques.	Liste			
ListRobots	Répertorie les robots.	Liste			
ListSimulationApplications	Répertorie les applications de simulation.	Liste			
ListSimulationJobBatches	Répertorie les lots de tâches de simulation	Liste			
ListSimulationJobs	Répertorie les tâches de simulation.	Liste			
ListSupportedAvailabilityZones [autorisation uniquement]	Répertorie les zones de disponibilité prises en charge.	List			
ListTagsForResource	Répertorier les balises d'une RoboMaker ressource	List	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
ListWorldExportJobs	Répertorie les tâches d'exportation d'environnement.	Liste			
ListWorldGenerationJobs	Répertorie les tâches de génération d'environnement.	Liste			
ListWorldTemplates	Répertorie les modèles d'environnement.	Liste			
ListWorlds	Répertorie les environnements.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterRobot	Enregistre un robot dans une flotte.	Écriture	deploymentFleet*		
			robot*		
RestartSimulationJob	Redémarre une tâche de simulation en cours d'exécution.	Écriture	simulationJob*		
StartSimulationJobBatch	Crée un lot de tâches de simulation	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
SyncDeploymentJob	Garantit que l'application robotique déployée le plus récemment est déployée sur tous les robots de la flotte.	Écrire	deploymentFleet*		iam:CreateServiceLinkedRole
TagResource	Ajouter des balises à une RoboMaker ressource	Identification	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Supprimer les balises d'une RoboMaker ressource	Identification	deploymentFleet		
			deploymentJob		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys	
UpdateRobotApplication	Met à jour une application robotique	Écriture	robotApplication*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRobotDeployment [autorisation uniquement]	Signale l'état de déploiement d'un robot.	Écriture			
UpdateSimulationApplication	Met à jour une application de simulation.	Écriture	simulationApplication*		
UpdateWorldTemplate	Met à jour un modèle d'environnement.	Écrire	worldTemplate*		

Types de ressources définis par AWS RoboMaker

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
robotApplication	`arn:${Partition}:robomaker:${Region}:${Account}:robot-application/${ApplicationName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey}
simulationApplication	`arn:${Partition}:robomaker:${Region}:${Account}:simulation-application/${ApplicationName}/${CreatedOnEpoch}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
simulationJob	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job/${SimulationJobId}	aws:ResourceTag/${TagKey}
simulationJobBatch	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job-batch/${SimulationJobBatchId}	aws:ResourceTag/${TagKey}
deploymentJob	arn:${Partition}:robomaker:${Region}:${Account}:deployment-job/${DeploymentJobId}	aws:ResourceTag/${TagKey}
robot	arn:${Partition}:robomaker:${Region}:${Account}:robot/${RobotName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
deploymentFleet	arn:${Partition}:robomaker:${Region}:${Account}:deployment-fleet/${FleetName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
worldGenerationJob	arn:${Partition}:robomaker:${Region}:${Account}:world-generation-job/${WorldGenerationJobId}	aws:ResourceTag/${TagKey}
worldExportJob	arn:${Partition}:robomaker:${Region}:${Account}:world-export-job/${WorldExportJobId}	aws:ResourceTag/${TagKey}
worldTemplate	arn:${Partition}:robomaker:${Region}:${Account}:world-template/${WorldTemplateJobId}	aws:ResourceTag/${TagKey}
world	arn:${Partition}:robomaker:${Region}:${Account}:world/${WorldId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS RoboMaker

AWS RoboMaker définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Route 53

Amazon Route 53 (préfixe de service : `route53`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Route 53

- Types de ressources définis par Amazon Route 53
- Clés de condition pour Amazon Route 53

Actions définies par Amazon Route 53

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateKeySigningKey	Accorde l'autorisation d'activer une clé de signature de clé afin qu'elle puisse être utilisée pour la signature par DNSSEC	Écriture	hostedzone*		
AssociateVPCWithHostedZone	Accorde l'autorisation d'associer un Amazon VPC supplémentaire à une zone hébergée privée.	Écrire	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
ChangeCidrCollection	Accorde l'autorisation de créer ou de supprimer des blocs CIDR dans une collection CIDR	Écrire	cidrcollection*		
ChangeResourceRecordSets	Accorde l'autorisation de créer, mettre à jour et supprimer un enregistrement contenant des informations DNS faisant autorité pour un	Écriture	hostedzone*		
				route53:ChangeResc	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	nom de domaine ou de sous-domaine spécifié.			urceRecordSetsNormalizedRecordNames route53:ChangeResourceRecordSetsRecordTypes route53:ChangeResourceRecordSetsActions	
ChangeTagsForResource	Accorde l'autorisation d'ajouter, de modifier ou de supprimer des balises pour une vérification de l'état ou une zone hébergée.	Identification	healthcheck* hostedzone*		
CreateCidrCollection	Accorde l'autorisation de créer une nouvelle collection CIDR	Écrire			
CreateHealthCheck	Accorde l'autorisation de créer une nouvelle vérification de l'état, qui surveille l'état et les performances de vos applications web, de vos serveurs web et d'autres ressources.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateHostedZone	Accorde l'autorisation de créer une zone hébergée publique pour spécifier la façon dont le système de noms de domaine (DNS) achemine le trafic sur Internet pour un domaine, tel que exemple.com, et ses sous-domaines.	Écriture		route53:VPCs	ec2:DescribeVpcs
CreateKeySigningKey	Accorde l'autorisation de créer une clé de signature de clé associée à une zone hébergée	Écriture	hostedzone*		
CreateQueryLoggingConfig	Accorde l'autorisation de créer une configuration pour la journalisation des requêtes DNS.	Écriture	hostedzone*		
CreateReusableDelegationSet	Accorde l'autorisation de créer un ensemble de délégations (groupe de quatre serveurs de noms) qui peut être réutilisé par plusieurs zones hébergées .	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTrafficPolicy	Accorde l'autorisation de créer une politique de trafic pour créer plusieurs enregistrements DNS pour un nom de domaine unique (par exemple, exemple.com) ou un nom de sous-domaine unique (par exemple, www.exemple.com).	Écriture			
CreateTrafficPolicyInstance	Accorde l'autorisation de créer des enregistrements dans une zone hébergée spécifiée en fonction des paramètres figurant dans une version de politique de trafic spécifiée.	Écriture	hostedzone* trafficpolicy*		
CreateTrafficPolicyVersion	Accorde l'autorisation de créer une nouvelle version d'une politique de trafic existante.	Écrire	trafficpolicy*		
CreateVPCAssociationAuthorization	Accorde l'autorisation d'autoriser le VPC Compte AWS qui a créé un VPC spécifié à soumettre une VPCWith HostedZone demande d'associé, qui associe le VPC à une zone hébergée spécifiée créée par un autre compte	Écrire	hostedzone* 	 route53:VPCs	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeactivateKeySigningKey	Accorde l'autorisation de désactiver une clé de signature de clé afin qu'elle ne soit pas utilisée pour la signature par DNSSEC	Écrire	hostedzone*		
DeleteCidrCollection	Accorde l'autorisation de supprimer une collection CIDR	Écrire	cidrcollection*		
DeleteHealthCheck	Accorde l'autorisation de supprimer une vérification de l'état.	Écriture	healthcheck*		
DeleteHostedZone	Accorde l'autorisation de supprimer une zone hébergée.	Écriture	hostedzone*		
DeleteKeySigningKey	Accorde l'autorisation de supprimer une clé de signature de clé	Écriture	hostedzone*		
DeleteQueryLoggingConfig	Accorde l'autorisation de supprimer une configuration pour la journalisation des requêtes DNS.	Écriture	queryloggingconfig*		
DeleteReusableDelegationSet	Accorde l'autorisation de supprimer un ensemble de délégations réutilisables.	Écriture	delegationset*		
DeleteTrafficPolicy	Accorde l'autorisation de supprimer une politique de trafic.	Écriture	trafficpolicy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTrafficPolicyInstance	Accorde l'autorisation de supprimer une instance de politique de trafic et tous les enregistrements que Route 53 a créés lorsque vous avez créé l'instance.	Écriture	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	Accorde l'autorisation de supprimer l'autorisation d'associer un Amazon Virtual Private Cloud à une zone hébergée privée Route 53.	Écriture	hostedzone*		
				route53:VPCs	
DisableHostedZoneDNSSEC	Accorde l'autorisation de désactiver la signature DNSSEC dans une zone hébergée spécifique	Écriture	hostedzone*		
DisassociateVPCFromHostedZone	Accorde l'autorisation de dissocier un Amazon Virtual Private Cloud d'une zone hébergée privée Route 53.	Écriture	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
EnableHostedZoneDNSSEC	Accorde l'autorisation d'activer la signature DNSSEC dans une zone hébergée spécifique	Écriture	hostedzone*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountLimit	Accorde l'autorisation d'obtenir la limite spécifiée pour le compte actuel, par exemple, le nombre maximal de vérifications de l'état que vous pouvez créer à l'aide du compte.	Lecture			
GetChange	Accorde l'autorisation d'obtenir le statut actuel d'une demande pour créer, mettre à jour ou supprimer un ou plusieurs enregistrements.	Liste	change*		
GetCheckerIpRanges	Accorde l'autorisation d'obtenir la liste des plages d'adresses IP qui sont utilisées par les outils de vérification de l'état Route 53 pour vérifier l'état de vos ressources	Liste			
GetDNSSEC	Accorde l'autorisation de récupérer des informations sur DNSSEC pour une zone hébergée spécifique, y compris les clés de signature de la zone hébergée	Lecture	hostedzone*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGeoLocation	Accorde l'autorisation d'obtenir des informations concernant la prise en charge ou non d'un emplacement géographique spécifié pour les enregistrements de géolocalisation Route 53.	Liste			
GetHealthCheck	Accorde l'autorisation d'obtenir des informations sur une vérification de l'état spécifiée.	Lecture	healthcheck*		
GetHealthCheckCount	Accorde l'autorisation d'obtenir le nombre de bilans de santé associés au Compte AWS	List			
GetHealthCheckLastFailureReason	Accorde l'autorisation d'obtenir la raison pour laquelle une vérification de l'état spécifiée a échoué dernièrement.	Liste	healthcheck*		
GetHealthCheckStatus	Accorde l'autorisation d'obtenir le statut d'une vérification de l'état spécifiée.	Liste	healthcheck*		
GetHostedZone	Accorde l'autorisation d'obtenir des informations sur une zone hébergée spécifiée, y compris les quatre serveurs de noms que Route 53 a affectés à la zone hébergée.	List	hostedzone*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetHostedZoneCount	Accorde l'autorisation d'obtenir le nombre de zones hébergées associées au Compte AWS	List			
GetHostedZoneLimit	Accorde l'autorisation d'obtenir la limite spécifiée pour une zone hébergée spécifiée.	Lecture	hostedzone*		
GetQueryLoggingConfig	Accorde l'autorisation d'obtenir des informations sur une configuration spécifiée pour la journalisation des requêtes DNS.	Lecture	queryloggingconfig*		
GetReusableDelegationSet	Accorde l'autorisation d'obtenir des informations sur un ensemble de délégations réutilisables spécifié, y compris les quatre serveurs de noms affectés à l'ensemble de délégations.	Liste	delegationset*		
GetReusableDelegationSetLimit	Accorde l'autorisation d'obtenir le nombre maximal de zones hébergées que vous pouvez associer à l'ensemble de délégations réutilisables spécifié.	Lecture	delegationset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTrafficPolicy	Accorde l'autorisation d'obtenir des informations sur une version de politique de trafic spécifiée.	Lecture	trafficpolicy*		
GetTrafficPolicyInstance	Accorde l'autorisation d'obtenir des informations sur une instance de politique de trafic spécifiée.	Lecture	trafficpolicyinstance*		
GetTrafficPolicyInstanceCount	Accorde l'autorisation d'obtenir le nombre d'instances de politique de trafic associées au Compte AWS	Lecture			
ListCidrBlocks	Accorde l'autorisation d'obtenir une liste des blocs CIDR dans une collection CIDR spécifiée	List	cidrcollection*		
ListCidrCollections	Accorde l'autorisation d'obtenir une liste des collections CIDR associées au Compte AWS	List			
ListCidrLocations	Accorde l'autorisation d'obtenir une liste des emplacements CIDR qui appartiennent à une collection CIDR spécifiée	List	cidrcollection*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGeoLocations	Accorde l'autorisation d'obtenir la liste des emplacements géographiques que Route 53 prend en charge pour la géolocalisation.	Lecture			
ListHealthChecks	Accorde l'autorisation d'obtenir une liste des bilans de santé associés au Compte AWS	Lecture			
ListHostedZones	Accorde l'autorisation d'obtenir une liste des zones hébergées publiques et privées associées au Compte AWS	List			
ListHostedZonesByName	Accorde l'autorisation d'obtenir la liste de vos zones hébergées dans un ordre lexicographique. Les zones hébergées sont triées par nom avec les étiquettes inversées, par exemple, com.example.www	List			
ListHostedZonesByVPC	Accorde l'autorisation d'obtenir une liste de toutes les zones hébergées privées auxquelles un VPC spécifié est associé.	List		route53:VPCs	ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListQueryLoggingConfigs	Accorde l'autorisation de répertorier les configurations pour la journalisation des requêtes DNS associées à la configuration actuelle Compte AWS ou à la configuration associée à une zone hébergée spécifiée	List	hostedzone		
ListResourceRecordSets	Accorde l'autorisation de répertorier les enregistrements dans une zone hébergée spécifiée.	List	hostedzone*		
ListReusableDelegationSets	Accorde l'autorisation de répertorier les ensembles de délégations réutilisables qui sont associés au Compte AWS actuel.	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour une surveillance de l'état ou une zone hébergée.	Lecture	healthcheck		
			hostedzone		
ListTagsForResources	Accorde l'autorisation de répertorier les balises pour 10 surveillances de l'état ou zones hébergées au plus.	Lecture	healthcheck		
			hostedzone		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTrafficPolicies	Accorde l'autorisation d'obtenir des informations sur la version la plus récente pour chaque politique de trafic qui est associée au Compte AWS actuel. Les stratégies sont répertoriées dans l'ordre où elles ont été créées	List			
ListTrafficPolicyInstances	Accorde l'autorisation d'obtenir des informations sur les instances de politique de trafic que vous avez créées à l'aide du Compte AWS	Lecture			
ListTrafficPolicyInstancesByHostedZone	Accorde l'autorisation d'obtenir des informations sur les instances de politique de trafic que vous avez créées dans une zone hébergée spécifiée.	Liste	hostedzone*		
ListTrafficPolicyInstancesByPolicy	Accorde l'autorisation d'obtenir des informations sur les instances de politique de trafic que vous avez créées à l'aide d'une version de politique de trafic spécifiée.	Liste	trafficpolicy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTrafficPolicyVersions	Accorde l'autorisation d'obtenir des informations sur toutes les versions d'une politique de trafic spécifiée.	List	trafficpolicy*		
ListVPCAssociationAuthorizations	Accorde l'autorisation d'obtenir une liste des VPCs comptes créés par d'autres comptes et pouvant être associés à une zone hébergée spécifiée	List	hostedzone*		
TestDNSAnswer	Accorde l'autorisation d'obtenir la valeur que Route 53 renvoie en réponse à une requête DNS pour un nom et un type d'enregistrement spécifiés.	Lecture			
UpdateHealthCheck	Accorde l'autorisation de mettre à jour une vérification de l'état existante.	Écriture	healthcheck*		
UpdateHostedZoneComment	Accorde l'autorisation de mettre à jour le commentaire pour une zone hébergée spécifiée.	Écrire	hostedzone*		
UpdateHostedZoneFeatures	Autorise la mise à jour des fonctionnalités pour une zone hébergée spécifiée	Écrire	hostedzone*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTrafficPolicyComment	Accorde l'autorisation de mettre à jour le commentaire pour une version de politique de trafic spécifiée.	Écriture	trafficpolicy*		
UpdateTrafficPolicyInstance	Accorde l'autorisation de mettre à jour les enregistrements d'une zone hébergée spécifiée qui ont été créés en fonction des paramètres figurant dans une version de politique de trafic spécifiée.	Écriture	trafficpolicyinstance*		

Types de ressources définis par Amazon Route 53

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cidrcollection	`arn:${Partition}:route53:::cidrcollection/${Id}`	
change	`arn:${Partition}:route53:::change/${Id}`	

Types de ressources	ARN	Clés de condition
delegationset	arn:${Partition}:route53:::delegationset/${Id}	
healthcheck	arn:${Partition}:route53:::healthcheck/${Id}	
hostedzone	arn:${Partition}:route53:::hostedzone/${Id}	
trafficpolicy	arn:${Partition}:route53:::trafficpolicy/${Id}	
trafficpolicyinstance	arn:${Partition}:route53:::trafficpolicyinstance/${Id}	
queryloggingconfig	arn:${Partition}:route53:::queryloggingconfig/${Id}	
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	

Clés de condition pour Amazon Route 53

Amazon Route 53 définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
route53:ChangeResourceRecordSetsActions	Filtre l'accès par les actions de modification CREATE, UPSERT ou DELETE contenues dans une demande ChangeResourceRecordSets	ArrayOfString
route53:ChangeResourceRecordSetsNormalizedRecordNames	Filtre l'accès en fonction des noms d'enregistrement DNS normalisés dans une demande ChangeResourceRecordSets	ArrayOfString
route53:ChangeResourceRecordSetsRecordTypes	Filtre l'accès en fonction du type d'enregistrement DNS dans une ChangeResourceRecordSets demande	ArrayOfString
route53:VPCs	Filtre l'accès VPCs en fonction de la demande	String

Actions, ressources et clés de condition pour Amazon Route 53 Domains

Amazon Route 53 Domains (préfixe de service : `route53domains`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Route 53 Domains

- Types de ressources définis par Amazon Route 53 Domains
- Clés de condition pour Amazon Route 53 Domains

Actions définies par Amazon Route 53 Domains

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptDomainTransferFromAnotherAwsAccount	Accorde l'autorisation d'accepter le transfert d'un domaine d'un autre Compte AWS vers le domaine actuel Compte AWS	Écrire			
AssociateDelegationSignerToDomain	Accorde l'autorisation d'associer un nouveau signataire de délégation à un domaine	Écrire			
CancelDomainTransferToAnotherAwsAccount	Accorde l'autorisation d'annuler le transfert d'un domaine de l'actuel Compte AWS vers un autre Compte AWS	Écrire			
CheckDomainAvailability	Accorde l'autorisation de vérifier la disponibilité d'un nom de domaine.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CheckDomainTransferability	Accorde l'autorisation de vérifier si un nom de domaine peut être transféré vers Amazon Route 53	Lecture			
DeleteDomain	Accorde l'autorisation de supprimer des domaines	Écrire			
DeleteTagsForDomain	Accorde l'autorisation de supprimer les balises spécifiées pour un domaine.	Balisage			
DisableDomainAutoRenew	Accorde l'autorisation de configurer Amazon Route 53 pour renouveler automatiquement le domaine spécifié avant que son enregistrement n'arrive à expiration.	Écrire			
DisableDomainTransferLock	Accorde l'autorisation de supprimer le verrou de transfert sur le domaine (en particulier le clientTransferProhibited statut) pour autoriser les transferts de domaine	Écrire			
DisassociateDelegationSignerFromDomain	Accorde l'autorisation de dissocier un signataire de délégation existant d'un domaine	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableDomainAutoRenew	Accorde l'autorisation de configurer Amazon Route 53 pour renouveler automatiquement le domaine spécifié avant que son enregistrement n'arrive à expiration.	Écrire			
EnableDomainTransferLock	Accorde l'autorisation de définir le verrou de transfert sur le domaine (en particulier le clientTransferProhibited statut) afin d'empêcher les transferts de domaine	Écrire			
GetContactReachabilityStatus	Accorde l'autorisation de renvoyer des informations indiquant si le contact inscrit a répondu pour les opérations qui nécessitent une confirmation de la validité de l'adresse e-mail du contact inscrit, tels que l'enregistrement d'un nouveau domaine	Lecture			
GetDomainDetail	Accorde l'autorisation d'obtenir des informations détaillées sur un domaine.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDomainSuggestions	Accorde l'autorisation de renvoyer la liste des noms de domaine suggérés à partir d'une chaîne, qui peut être un nom de domaine ou simplement un mot ou une expression (sans espaces).	Lecture			
GetOperationDetail	Accorde l'autorisation d'obtenir l'état actuel d'une opération qui n'est pas terminée.	Lecture			
ListDomains	Accorde l'autorisation de répertorier tous les noms de domaine enregistrés auprès d'Amazon Route 53 pour le moment Compte AWS	List			
ListOperations	Accorde l'autorisation IDs de répertorier les opérations qui ne sont pas encore terminées	List			
ListPrices	Donne l'autorisation de répertorier les prix des opérations pour TLDs	List			
ListTagsForDomain	Accorde l'autorisation de répertorier toutes les balises qui sont associées au domaine spécifié.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PushDomain	Accorde l'autorisation de modifier la balise IPS du domaine .uk pour lancer un processus de transfert de Route 53 vers un autre bureau d'enregistrement	Écrire			
RegisterDomain	Accorde l'autorisation d'enregistrer des domaines.	Écrire			
RejectDomainTransferFromAnotherAwsAccount	Accorde l'autorisation de refuser le transfert d'un domaine d'un autre Compte AWS vers le domaine actuel Compte AWS	Écrire			
RenewDomain	Accorde l'autorisation de renouveler les domaines pour le nombre d'années spécifié.	Écrire			
ResendContactReachabilityEmail	Accorde l'autorisation de renvoyer l'e-mail de confirmation à l'adresse électronique actuelle du contact inscrit pour les opérations qui nécessitent une confirmation de la validité de l'adresse e-mail du contact inscrit, tels que l'enregistrement d'un nouveau domaine	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResendOperationAuthorization	Accorde l'autorisation de renvoyer l'autorisation d'opération	Écrire			
RetrieveDomainAuthCode	Accorde l'autorisation d'obtenir le AuthCode pour le domaine	Écrire			
TransferDomain	Accorde l'autorisation de transférer un domaine d'un autre serveur d'inscriptions vers Amazon Route 53.	Écrire			
TransferDomainToAnotherAwsAccount	Accorde l'autorisation de transférer un domaine de l'actuel Compte AWS à un autre Compte AWS	Écrire			
UpdateDomainContact	Accorde l'autorisation de mettre à jour les informations de contact pour un domaine.	Écriture			
UpdateDomainContactPrivacy	Accorde l'autorisation de mettre à jour les paramètres de confidentialité de contact.	Écriture			
UpdateDomainNameservers	Accorde l'autorisation de remplacer l'ensemble actuel des serveurs de noms pour un domaine avec l'ensemble de serveurs de noms spécifié.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTagsForDomain	Accorde l'autorisation d'ajouter ou de mettre à jour des balises pour un domaine spécifié.	Identification			
ViewBilling	Accorde l'autorisation d'obtenir tous les enregistrements de facturation relatifs au domaine pour le moment Compte AWS pendant une période spécifiée	Lecture			

Types de ressources définis par Amazon Route 53 Domains

Amazon Route 53 Domains ne prend pas en charge la spécification d'un ARN de ressource dans l'élément `Resource` d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon Route 53 Domains, spécifiez `"Resource": "*"` dans votre stratégie.

Clés de condition pour Amazon Route 53 Domains

Route 53 Domains ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les profils Amazon Route 53

Les profils Amazon Route 53 (préfixe de service :`route53profiles`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les profils Amazon Route 53
- Types de ressources définis par les profils Amazon Route 53
- Clés de condition pour les profils Amazon Route 53

Actions définies par les profils Amazon Route 53

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate Profile	Accorde l'autorisation d'associer un profil au VPC du client	Écrire		aws:RequestTag/${TagKey} aws:TagKeys route53profiles:ResourceIds	ec2:DescribeVpcs
Associate ResourceToProfile	Accorde l'autorisation d'associer une ressource, telle qu'un groupe de règles de pare-feu DNS, une zone	Écrire		route53profiles:ResourceTypes	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	hébergée privée, une règle de résolution, etc., à un profil spécifié			route53profiles:HostedZoneDomains route53profiles:ResolverRuleDomains route53profiles:FirewallRuleGroupPriority route53profiles:ResourceArns	
CreateProfile	Accorde l'autorisation de créer une nouvelle ressource de profil	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteProfile	Accorde l'autorisation de supprimer un profil spécifié par le ProfileId	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateProfile	Accorde l'autorisation de supprimer une association entre un VPC client et le profil spécifié	Écrire		route53profiles:ResourceIds	
DisassociateResourceFromProfile	Accorde l'autorisation de supprimer l'association entre la ressource, telle qu'un groupe de règles de pare-feu DNS, une zone hébergée privée, une règle de résolution, etc., et le profil spécifié	Écrire		route53profiles:ResourceTypes route53profiles:HostedZoneDomains route53profiles:ResolverRuleDomains route53profiles:FirewallRuleGroupPriority route53profiles:ResourceArns	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProfile	Accorde l'autorisation d'obtenir un profil	Lecture			
GetProfileAssociation	Accorde l'autorisation d'obtenir un profil à une association VPC spécifiée par l'ID d'association de profil	Lecture			
GetProfilePolicy [autorisation uniquement]	Accorde l'autorisation de lire la politique de contrôle d'accès à la RAM pour un profil	Lecture	profile*		
GetProfileResourceAssociation	Accorde l'autorisation d'obtenir une association de ressources Profile sur la base de ProfileResourceAssociationId	Lecture			
ListProfileAssociations	Accorde l'autorisation de répertorier tous VPCs les profils spécifiés associés à	List			
ListProfileResourceAssociations	Permet de répertorier toutes les associations entre les ressources, telles que les groupes de règles du pare-feu DNS, les zones hébergées privées, les règles de résolution, etc. pour l'ID de profil donné	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProfiles	Autorise le client à répertorier tous les profils créés et partagés avec lui	List			
ListTagsForResource	Accorde l'autorisation de répertorier tous les tags associés à la ressource	List			
PutProfilePolicy [autorisation uniquement]	Accorde l'autorisation de définir la politique de contrôle d'accès à la RAM pour un profil	Écrire	profile*		
TagResource	Accorde l'autorisation d'ajouter un tag à la ressource donnée	Identification	profile		
			profile-association		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer un tag de la ressource donnée	Identification	profile		
			profile-association		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateProfileResourceAssociation	Accorde l'autorisation de mettre à jour le nom de l'association de ressources Profile ou les propriétés de la ressource, ou les deux. Si le nom et les propriétés de ressource sont nuls, l'API renvoie l'association de ressources Profile existante	Écrire		route53profiles:ResourceTypes route53profiles:HostedZoneDomains route53profiles:ResolverRuleDomains route53profiles:FirewallRuleGroupPriority	

Types de ressources définis par les profils Amazon Route 53

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
profile	`arn:${Partition}:route53profiles:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
profile-association	`arn:${Partition}:route53profiles:${Region}:${Account}:profile-association/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les profils Amazon Route 53

Les profils Amazon Route 53 définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Clés de condition	Description	Type
route53profiles:FirewallRuleGroupPriority	Filtre l'accès par plage de priorités d'un groupe de règles de pare-feu	Numérique
route53profiles:HostedZoneDomains	Filtre l'accès par domaines de zone hébergée	String
route53profiles:ResolverRuleDomains	Filtre l'accès par domaines Resolver Rule	String
route53profiles:ResourceArns	Filtre l'accès par ressource spécifique ARNs	ARN
route53profiles:ResourceIds	Filtre l'accès par donnée VPCs	String
route53profiles:ResourceTypes	Filtre l'accès par type de ressource spécifique. Les options possibles incluent HostedZone « », FirewallRuleGroup « », ResolverQueryLoggingConfig « », ResolverRule « » et « VpcEndpoint »	String

Actions, ressources et clés de condition pour Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster (préfixe de service : `route53-recovery-cluster`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Route 53 Recovery Cluster
- Types de ressources définis par Amazon Route 53 Recovery Cluster
- Clés de condition pour Amazon Route 53 Recovery Cluster

Actions définies par Amazon Route 53 Recovery Cluster

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRoutingControlState	Accorde l'autorisation d'obtenir un état de contrôle de routage	Lecture	routingcontrol*		
ListRoutingControls	Accorde l'autorisation de répertorier les contrôles de routage	Lecture			
UpdateRoutingControlState	Accorde l'autorisation de mettre à jour un état de contrôle de routage	Écrire	routingcontrol*		
				route53-recovery-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				cluster:AllowSafetyRulesOverrides	
UpdateRoutingControlStates	Accorde l'autorisation de mettre à jour un lot d'états de contrôle de routage	Écrire	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	

Types de ressources définis par Amazon Route 53 Recovery Cluster

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	

Clés de condition pour Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
route53-recovery-cluster:AllowSafetyRulesOverrides	Remplacer les règles de sécurité pour autoriser les mises à jour de l'état du contrôle du routage	Booléen

Actions, ressources et clés de condition pour Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls (préfixe de service : `route53-recovery-control-config`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Route 53 Recovery Controls
- Types de ressources définis par Amazon Route 53 Recovery Controls
- Clés de condition pour Amazon Route 53 Recovery Controls

Actions définies par Amazon Route 53 Recovery Controls

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCluster	Accorde l'autorisation de créer un cluster	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateControlPanel	Accorde l'autorisation de créer un panneau de configuration	Écrire	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoutingControl	Accorde l'autorisation de créer un contrôle de routage	Écrire	cluster*		
CreateSafetyRule	Accorde l'autorisation de créer une règle de sécurité	Écrire	cluster*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DeleteCluster	Accorde l'autorisation de supprimer un cluster	Écrire	cluster*		
DeleteControlPanel	Accorde l'autorisation de supprimer un panneau de configuration	Écrire	controlpanel*		
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer la politique de contrôle d'accès à la RAM pour un cluster	Gestion des autorisations	cluster*		
DeleteRoutingControl	Accorde l'autorisation de supprimer un contrôle de routage	Écriture	routingcontrol*		
DeleteSafetyRule	Accorde l'autorisation de supprimer une règle de sécurité	Écriture	safetyrule*		
DescribeCluster	Accorde l'autorisation de décrire un cluster	Read	cluster*		
DescribeControlPanel	Accorde l'autorisation de décrire un panneau de configuration	Read	controlpanel*		
DescribeRoutingControl	Accorde l'autorisation de décrire un contrôle de routage	Read	routingcontrol*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSafetyRule	Accorde l'autorisation de décrire une règle de sécurité	Lecture	safetyrule*		
GetResourcePolicy	Accorde l'autorisation d'obtenir la stratégie de ressource d'un cluster.	Lecture	cluster*		
ListAssociatedRoute53HealthChecks	Accorde l'autorisation de répertorier les surveillances de l'état Route 53 associées	List	routingcontrol*		
ListClusters	Accorde l'autorisation de répertorier les clusters virtuels	Lecture			
ListControlPanels	Accorde l'autorisation de répertorier les panneaux de configuration	Read			
ListRoutingControls	Accorde l'autorisation de répertorier les contrôles de routage	Lecture	controlpanel*		
ListSafetyRules	Accorde l'autorisation de répertorier les règles de sécurité	Lecture	controlpanel*		
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture	cluster		
			controlpanel		
			safetyrule		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de définir la politique de contrôle d'accès à la RAM pour un cluster	Gestion des autorisations	cluster*		
TagResource	Accorde l'autorisation de baliser une ressource	Identification	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys	
UpdateCluster	Accorde l'autorisation de mettre à jour un cluster	Écrire	cluster*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateControlPanel	Accorde l'autorisation de mettre à jour un cluster	Écrire	controlpanel*		
UpdateRoutingControl	Accorde l'autorisation de mettre à jour un contrôle de routage	Écrire	routingcontrol*		
UpdateSafetyRule	Accorde l'autorisation de mettre à jour une règle de sécurité	Écrire	safetyrule*		

Types de ressources définis par Amazon Route 53 Recovery Controls

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cluster	`arn:${Partition}:route53-recovery-control::${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
controlpanel	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
routingcontrol	arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}	
safetyrule	arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/safetyrule/${SafetyRuleId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Route 53 Recovery Readiness

Amazon Route 53 Recovery Readiness (préfixe de service : `route53-recovery-readiness`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Route 53 Recovery Readiness
- Types de ressources définis par Amazon Route 53 Recovery Readiness
- Clés de condition pour Amazon Route 53 Recovery Readiness

Actions définies par Amazon Route 53 Recovery Readiness

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCell	Accorde l'autorisation de créer une cellule	Écrire	cell*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateCrossAccountAuthorization	Accorde l'autorisation de créer une autorisation multicomptes	Écrire			
CreateReadinessCheck	Accorde l'autorisation de créer une vérification de l'état de préparation	Écrire	readinesscheck*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryGroup	Accorde l'autorisation de créer un groupe de récupération	Écrire	recoverygroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceSet	Accorde l'autorisation de créer un ensemble de ressources	Écrire	resourceset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCell	Accorde l'autorisation de supprimer une cellule	Écrire	cell*		
DeleteCrossAccountAuthorization	Accorde l'autorisation de supprimer une autorisation multicomptes	Écrire			
DeleteReadinessCheck	Accorde l'autorisation de supprimer une vérification de l'état de préparation	Écrire	readinesscheck*		
DeleteRecoveryGroup	Accorde l'autorisation de supprimer un groupe de récupération	Écrire	recoverygroup*		
DeleteResourceSet	Accorde l'autorisation de supprimer un ensemble de ressources	Écrire	resourceset*		
GetArchitectureRecommendations	Accorde l'autorisation d'obtenir des recommandations d'architecture pour un groupe de récupération	Lecture	recoverygroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCell	Accorde l'autorisation d'obtenir des informations sur une cellule	Lecture	cell*		
GetCellReadinessSummary	Accorde l'autorisation d'obtenir un résumé de l'état de préparation d'une cellule	Lecture	cell*		
GetReadinessCheck	Accorde l'autorisation d'obtenir des informations sur une vérification de l'état de préparation	Lecture	readinesscheck*		
GetReadinessCheckResourceStatus	Accorde l'autorisation d'obtenir l'état de préparation d'une ressource individuelle	Lecture	readinesscheck*		
GetReadinessCheckStatus	Accorde l'autorisation d'obtenir l'état de vérification de préparation (d'un ensemble de ressources)	Lecture	readinesscheck*		
GetRecoveryGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de récupération	Lecture	recoverygroup*		
GetRecoveryGroupReadinessSummary	Accorde l'autorisation d'obtenir le résumé de l'état de préparation d'un groupe de récupération	Lecture	recoverygroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourceSet	Accorde l'autorisation d'obtenir des informations sur un ensemble de ressources	Lecture	resourceset*		
ListCells	Accorde l'autorisation de répertorier des cellules	Lecture			
ListCrossAccountAuthorizations	Accorde l'autorisation de répertorier les autorisations multicomptes	Lecture			
ListReadinessChecks	Accorde l'autorisation de répertorier les vérifications de préparation	Lecture			
ListRecoveryGroups	Accorde l'autorisation de répertorier les groupes de récupération	Lecture			
ListResourceSets	Accorde l'autorisation de répertorier les ensembles de ressources	Lecture			
ListRules	Accorde l'autorisation de répertorier les règles de préparation	Read			
ListTagsForResources	Accorde l'autorisation de répertorier les identifications d'une ressource	Read			
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource	Balisage	cell		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCell	Accorde l'autorisation de mettre à jour une cellule	Écrire	cell*		
				aws:TagKeys	
UpdateReadinessCheck	Accorde l'autorisation de mettre à jour une vérification de l'état de préparation	Écrire	readinesscheck*		
				aws:TagKeys	
UpdateRecoveryGroup	Accorde l'autorisation de mettre à jour un groupe de récupération	Écrire	recoverygroup*		
				aws:TagKeys	
UpdateResourceSet	Accorde l'autorisation de mettre à jour un ensemble de ressources	Écrire	resourceset*		
				aws:TagKeys	

Types de ressources définis par Amazon Route 53 Recovery Readiness

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
readiness check	arn:${Partition}:route53-recovery-readiness::${Account}:readiness-check/${ResourceId}	aws:ResourceTag/${TagKey}
resourceset	arn:${Partition}:route53-recovery-readiness::${Account}:resource-set/${ResourceId}	aws:ResourceTag/${TagKey}
cell	arn:${Partition}:route53-recovery-readiness::${Account}:cell/${ResourceId}	aws:ResourceTag/${TagKey}
recoverygroup	arn:${Partition}:route53-recovery-readiness::${Account}:recovery-group/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Route 53 Recovery Readiness

Amazon Route 53 Recovery Readiness définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Route 53 Resolver

Amazon Route 53 Resolver (préfixe de service : `route53resolver`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Route 53 Resolver
- Types de ressources définis par Amazon Route 53 Resolver
- Clés de condition pour Amazon Route 53 Resolver

Actions définies par Amazon Route 53 Resolver

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateFirewallRuleGroup	Accorde l'autorisation d'associer un VPC Amazon à un groupe de règles de pare-feu spécifié.	Écriture	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateResolverEndpointIpAddress	Accorde l'autorisation d'associer une adresse IP spécifiée à un point de terminaison Resolver. Il s'agit d'une adresse IP par laquelle les requêtes DNS transitent vers votre réseau (sortant) ou votre VPCs (entrant)	Écrire	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets
AssociateResolverQueryLogConfig	Accorde l'autorisation d'associer un VPC Amazon à une configuration de journalisation des requêtes spécifiée	Écriture	resolver-query-log-config*		ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateResolverRule	Accorde l'autorisation d'associer une règle Resolver spécifiée à un VPC spécifié.	Écriture	resolver-rule*		ec2:DescribeVpcs
CreateFirewallDomainList	Accorde l'autorisation de créer une liste de domaines de pare-feu.	Écriture	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Accorde l'autorisation de créer une règle de pare-feu dans un groupe de règles de pare-feu.	Écriture	firewall-domain-list*		
			firewall-rule-group*		
CreateFirewallRuleGroup	Accorde l'autorisation de créer un groupe de règles de pare-feu.	Écrire	firewall-rule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOutpostResolver	Octroie l'autorisation de créer un résolveur Route 53 sur Outposts.	Écrire	outpost-resolver*		outposts:GetOutpost
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverEndpoint	Accorde l'autorisation de créer un point de terminaison Resolver. Il existe deux types de points de terminaison Resolver : les points entrants et les points sortants	Écrire	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverQueryLogConfig	Accorde l'autorisation de créer une configuration de journalisation des requêtes Resolver, qui définit où vous souhaitez que Resolver enregistre les journaux de requêtes DNS provenant de votre VPCs	Écrire	resolver-query-log-config*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverRule	Accorde l'autorisation de définir la façon d'acheminer les requêtes arrivant hors du VPC.	Écrire	resolver-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewallDomainList	Accorde l'autorisation de supprimer une liste de domaines de pare-feu.	Écriture	firewall-domain-list*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFirewallRule	Accorde l'autorisation de supprimer une règle de pare-feu dans un groupe de règles de pare-feu.	Écriture	firewall-domain-list*		
			firewall-rule-group*		
DeleteFirewallRuleGroup	Accorde l'autorisation de supprimer un groupe de règles de pare-feu.	Écrire	firewall-rule-group*		
DeleteOutpostResolver	Octroie l'autorisation de supprimer un résolveur Route 53 sur Outposts.	Écrire	outpost-resolver*		
DeleteResolverEndpoint	Accorde l'autorisation de supprimer un point de terminaison Resolver. L'effet de la suppression d'un point de terminaison Resolver varie selon qu'il s'agit d'un point de terminaison entrant ou sortant	Écriture	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DeleteResolverQueryLogConfig	Accorde l'autorisation de supprimer une configuration de journalisation des requêtes Resolver	Écriture	resolver-query-log-config*		
DeleteResolverRule	Accorde l'autorisation de supprimer une règle Resolver	Écriture	resolver-rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateFirewallRuleGroup	Accorde l'autorisation de supprimer l'association entre un groupe de règles de pare-feu et un VPC spécifié.	Écriture	firewall-rule-group-association*		
DisassociateResolverEndpointIpAddress	Accorde l'autorisation de supprimer une adresse IP spécifiée à partir d'un point de terminaison Resolver. Il s'agit d'une adresse IP par laquelle les requêtes DNS transitent vers votre réseau (sortant) ou votre VPCs (entrant)	Écrire	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DisassociateResolverQueryLogConfig	Accorde l'autorisation de supprimer l'association entre une configuration de journalisation des requêtes Resolver spécifiée et un VPC spécifié	Écriture	resolver-query-log-config*		
DisassociateResolverRule	Accorde l'autorisation de supprimer l'association entre une règle Resolver et un VPC spécifié	Écriture	resolver-rule*		
GetFirewallConfig	Accorde l'autorisation d'obtenir des informations d'une configuration de pare-feu spécifiée.	Lecture	firewall-config*		ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFirewallDomainList	Accorde l'autorisation d'obtenir des informations sur une liste de domaines de pare-feu spécifiée.	Lecture	firewall-domain-list*		
GetFirewallRuleGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de règles de pare-feu spécifié.	Lecture	firewall-rule-group*		
GetFirewallRuleGroupAssociation	Accorde l'autorisation d'obtenir des informations sur une association entre un groupe de règles de pare-feu et un VPC.	Lecture	firewall-rule-group-association*		
GetFirewallRuleGroupPolicy	Accorde l'autorisation d'obtenir des informations sur une politique de groupe de règles de pare-feu spécifiée, qui spécifie les opérations et les ressources du groupe de règles de pare-feu que vous souhaitez autoriser un autre Compte AWS à utiliser	Lecture	firewall-rule-group*		
GetOutpostResolver	Octroie l'autorisation d'obtenir des informations sur un résolveur Route 53 spécifié sur Outposts.	Lecture	outpost-resolver*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResolverConfig	Accorde l'autorisation d'obtenir l'état de Resolver Config dans la ressource spécifiée	Lecture	resolver-config*		ec2:DescribeVpcs
GetResolverDnssecConfig	Accorde l'autorisation d'obtenir l'état de prise en charge de la validation DNSSEC pour les requêtes DNS au sein de la ressource spécifiée	Lecture	resolver-dnssec-config*		
GetResolverEndpoint	Accorde l'autorisation d'obtenir des informations sur un point de terminaison Resolver spécifié, par exemple s'il s'agit d'un point de terminaison Resolver entrant ou sortant, ainsi que les adresses IP de votre VPC vers lesquelles les requêtes DNS sont transférées lorsqu'elles arrivent sur votre VPC ou qu'elles le quittent	Lecture	resolver-endpoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResolverQueryLogConfig	Accorde l'autorisation d'obtenir des informations sur une configuration de journalisation des requêtes Resolver spécifiée, telles VPCs que le nombre de requêtes pour lesquelles la configuration enregistre les requêtes et l'emplacement vers lequel les journaux sont envoyés	Lecture	resolver-query-log-config*		ec2:DescribeVpcs
GetResolverQueryLogConfigAssociation	Accorde l'autorisation d'obtenir des informations sur une association spécifiée entre une configuration de journalisation des requêtes Resolver et un VPC Amazon. Lorsque vous associez un VPC à une configuration de journalisation des requêtes, Resolver consigne les requêtes DNS qui proviennent de ce VPC	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResolverQueryLogConfigPolicy	Accorde l'autorisation d'obtenir des informations sur une politique de journalisation des requêtes du résolveur spécifiée, qui spécifie les opérations de journalisation des requêtes du résolveur et les ressources que vous souhaitez autoriser un autre Compte AWS à utiliser	Lecture	resolver-query-log-config*		
GetResolverRule	Accorde l'autorisation d'obtenir des informations sur une règle Resolver spécifique, telle que le nom de domaine pour lequel la règle achemine les requêtes DNS et l'adresse IP vers laquelle les requêtes sont transférées.	Lecture	autodefined-rule		
			resolver-rule		
GetResolverRuleAssociation	Accorde l'autorisation d'obtenir des informations sur une association entre une règle Resolver et un VPC	Lecture	autodefined-rule		
			resolver-rule		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResolverRulePolicy	Accorde l'autorisation d'obtenir des informations sur une politique de règle du résolveur, qui spécifie les opérations et les ressources du résolveur que vous souhaitez autoriser un autre Compte AWS à utiliser	Lecture	resolver-rule*		
ImportFirewallDomains	Accorde l'autorisation d'ajouter, de supprimer ou de remplacer des domaines de pare-feu dans une liste de domaines de pare-feu.	Écrire	firewall-domain-list*		
ListFirewallConfigs	Accorde l'autorisation de répertorier toutes les configurations de pare-feu que la configuration actuelle Compte AWS est en mesure de vérifier	List			ec2:DescribeVpcs
ListFirewallDomainLists	Octroie l'autorisation de répertorier tous les domaines du pare-feu que la version actuelle Compte AWS est en mesure d'utiliser	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFirewallDomains	Accorde l'autorisation de répertorier tout le domaine du pare-feu dans une liste de domaines de pare-feu spécifiée	List	firewall-domain-list*		
ListFirewallRuleGroupAssociations	Accorde l'autorisation de répertorier les informations relatives aux associations entre Amazon VPCs et le groupe de règles Firewall	List			
ListFirewallRuleGroups	Accorde l'autorisation de répertorier tous les groupes de règles de pare-feu que le système actuel Compte AWS est en mesure d'utiliser	List			
ListFirewallRules	Accorde l'autorisation de répertorier toutes les règles de pare-feu sous un groupe de règles de pare-feu spécifié	List	firewall-rule-group*		
ListOutpostResolvers	Permet de répertorier toutes les instances de Route 53 Resolver sur les Outposts créées à l'aide du Compte AWS	List			
ListResolverConfigs	Accorde l'autorisation de répertorier les statuts de Resolver Config	List	resolver-config*		ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResolverDnssecConfigs	Accorde l'autorisation de répertorier l'état de prise en charge de la validation DNSSEC pour les requêtes DNS	List	resolver-dnssec-config*		
ListResolverEndpointIpAddresses	Accorde l'autorisation de répertorier les adresses IP transmises par les requêtes DNS sur le chemin de votre réseau (sortant) ou de votre réseau VPCs (entrant) pour un point de terminaison de résolution spécifié	List	resolver-endpoint*		
ListResolverEndpoints	Accorde l'autorisation de répertorier tous les points de terminaison du résolveur créés à l'aide du Compte AWS	List			
ListResolverQueryLogConfigAssociations	Accorde l'autorisation de répertorier des informations sur les associations entre Amazon VPCs et les configurations de journalisation des requêtes	List			ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResolverQueryLogConfigs	Accorde l'autorisation de répertorier les informations sur les configurations de journalisation des requêtes spécifiées, qui définissent l'endroit où vous souhaitez que Resolver enregistre les journaux de requêtes DNS et spécifient VPCs ceux pour lesquels vous souhaitez enregistrer les requêtes	List			ec2:DescribeVpcs
ListResolverRuleAssociations	Accorde l'autorisation de répertorier les associations créées entre les règles du résolveur et VPCs l'utilisation du Compte AWS	List			ec2:DescribeVpcs
ListResolverRules	Accorde l'autorisation de répertorier les règles du résolveur créées à l'aide du Compte AWS	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises que vous avez associées à la ressource spécifiée	Lecture	firewall-domain-list		
			firewall-rule-group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
PutFirewallRuleGroupPolicy	Accorde l'autorisation de spécifier un Compte AWS groupe de règles de pare-feu avec lequel vous souhaitez partager un groupe de règles de pare-feu, le groupe de règles de pare-feu que vous souhaitez partager et les opérations que vous souhaitez que le compte puisse effectuer sur la configuration	Gestion des autorisations	firewall-rule-group*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutResolverQueryLogConfigPolicy	Accorde l'autorisation de spécifier une Compte AWS configuration de journalisation des requêtes avec laquelle vous souhaitez partager une configuration de journalisation des requêtes, la configuration de journalisation des requêtes que vous souhaitez que le compte puisse effectuer sur la configuration	Gestion des autorisations	resolver-query-log-config*		
PutResolverRulePolicy	Accorde l'autorisation de spécifier les règles avec Compte AWS lesquelles vous souhaitez partager des règles, les règles du résolveur que vous souhaitez partager et les opérations que vous souhaitez que le compte puisse effectuer sur ces règles	Gestion des autorisations	resolver-rule*		
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à la ressource spécifiée	Balisage	firewall-config		
			firewall-domain-list		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises de la ressource spécifiée	Balisage	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateFirewallConfig	Accorde l'autorisation de mettre à jour des paramètres sélectionnés pour une configuration de pare-feu.	Écriture	firewall-config*		ec2:DescribeVpcs
UpdateFirewallDomains	Accorde l'autorisation d'ajouter, de supprimer ou de remplacer des domaines de pare-feu dans une liste de domaines de pare-feu.	Écriture	firewall-domain-list*		
UpdateFirewallRule	Accorde l'autorisation de mettre à jour des paramètres sélectionnés pour une règle de pare-feu dans un groupe de règles de pare-feu.	Écriture	firewall-domain-list*		
			firewall-rule-group*		
UpdateFirewallRuleGroupAssociation	Accorde l'autorisation de mettre à jour des paramètres sélectionnés pour une association de groupes de règles de pare-feu.	Écrire	firewall-rule-group-association*		
UpdateOutpostResolver	Octroie l'autorisation de mettre à jour les paramètres sélectionnés d'un résolveur Route 53 spécifié sur Outposts.	Écrire	outpost-resolver*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateResolverConfig	Accorde l'autorisation de mettre à jour l'état de Resolver Config dans la ressource spécifiée	Écrire	resolver-config*		ec2:DescribeVpcs
UpdateResolverDnssecConfig	Accorde l'autorisation de mettre à jour l'état de prise en charge de la validation DNSSEC pour les requêtes DNS au sein de la ressource spécifiée	Écriture	resolver-dnssec-config*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateResolverEndpoint	Accorde l'autorisation de mettre à jour les paramètres d'un point de terminaison Resolver entrant ou sortant.	Écriture	resolver-endpoint*		ec2:AssignIpv6Addresses ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyNetworkInterfaceAttribute ec2:UnassignIpv6Addresses
UpdateResolverRule	Accorde l'autorisation de mettre à jour les paramètres d'une règle Resolver spécifiée	Écriture	resolver-rule*		

Types de ressources définis par Amazon Route 53 Resolver

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
resolver-dnssec-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-dnssec-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-query-log-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-query-log-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-rule	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-rule/${ResourceId}	aws:ResourceTag/${TagKey}
autodefined-rule	arn:${Partition}:route53resolver:${Region}:${Account}:autodefined-rule/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-endpoint	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-endpoint/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-rule-group-association	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group-association/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-domain-list	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-domain-list/${ResourceId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
firewall-config	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-config/${ResourceId}	aws:ResourceTag/${TagKey}
resolver-config	arn:${Partition}:route53resolver:${Region}:${Account}:resolver-config/${ResourceId}	
outpost-resolver	arn:${Partition}:route53resolver:${Region}:${Account}:outpost-resolver/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Route 53 Resolver

Amazon Route 53 Resolver définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Route53 Global Resolver

AWS Route53 Global Resolver (préfixe de service :`route53globalresolver`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Route53 Global Resolver
- Types de ressources définis par AWS Route53 Global Resolver
- Clés de condition pour AWS Route53 Global Resolver

Actions définies par AWS Route53 Global Resolver

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource	Accorde l'autorisation de fournir des journaux pour un résolveur global	Gestion des autorisations	global-resolver*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
AssociateHostedZone	Accorde l'autorisation d'associer une ressource à une zone hébergée	Écrire			
BatchCreateFirewallRule	Autorise la création de plusieurs règles de pare-feu	Écrire			
BatchDeleteFirewallRule	Autorise la suppression de plusieurs règles de pare-feu	Écrire			
BatchUpdateFirewallRule	Autorise la mise à jour de plusieurs règles de pare-feu	Écrire			
CreateAccessSource	Accorde l'autorisation de créer une source d'accès	Écrire	dns-view*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccessToken	Accorde l'autorisation de créer un jeton d'accès	Écrire	access-token*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDNSView	Accorde l'autorisation de créer une vue DNS	Écrire	dns-view*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallDomainList	Accorde l'autorisation de créer une liste de domaines de pare-feu	Écrire	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Accorde l'autorisation de créer une règle de pare-feu	Écrire	dns-view*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			firewall-domain-list		
CreateGlobalResolver	Accorde l'autorisation de créer un résolveur global	Écrire	global-resolver*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessSource	Accorde l'autorisation de supprimer une source d'accès	Écrire	access-source*		
DeleteAccessToken	Accorde l'autorisation de supprimer un jeton d'accès	Écrire	access-token*		
DeleteDNSView	Autorise la suppression d'une vue DNS	Écrire	dns-view*		
DeleteFirewallDomainList	Autorise la suppression d'une liste de domaines de pare-feu	Écrire	firewall-domain-list*		
DeleteFirewallRule	Autorise la suppression d'une règle de pare-feu	Écrire			
DeleteGlobalResolver	Autorise la suppression d'un résolveur global	Écrire	global-resolver*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableDNSView	Accorde l'autorisation de désactiver une vue DNS	Écrire	dns-view*		
DisassociateHostedZone	Accorde l'autorisation de dissocier une zone hébergée d'une ressource	Écrire			
EnableDNSView	Accorde l'autorisation d'activer une vue DNS	Écrire	dns-view*		
GetAccessSource	Accorde l'autorisation d'obtenir une source d'accès	Lecture	access-source*		
GetAccessToken	Accorde l'autorisation d'obtenir un jeton d'accès	Lecture	access-token*		
GetDNSView	Accorde l'autorisation d'obtenir une vue DNS	Lecture	dns-view*		
GetFirewallDomainList	Accorde l'autorisation d'obtenir une liste de domaines de pare-feu	Lecture	firewall-domain-list*		
GetFirewallRule	Accorde l'autorisation d'obtenir une règle de pare-feu	Lecture			
GetGlobalResolver	Accorde l'autorisation d'obtenir un résolveur global	Lecture	global-resolver*		
GetHostedZoneAssociation	Accorde l'autorisation d'obtenir une association de zone hébergée	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetManagedFirewallDomainList	Accorde l'autorisation d'obtenir une liste de domaines de pare-feu gérés	Lecture			
ImportFirewallDomains	Accorde l'autorisation d'importer des domaines de pare-feu depuis un compartiment S3	Écrire	firewall-domain-list*		s3:GetObject s3:ListBucket
ListAccessSources	Accorde l'autorisation de répertorier les sources d'accès	List			
ListAccessTokens	Accorde l'autorisation de répertorier les jetons d'accès	List			
ListDNSViews	Accorde l'autorisation de répertorier les vues DNS	List			
ListFirewallDomainLists	Accorde l'autorisation de répertorier les listes de domaines du pare-feu	List			
ListFirewallDomains	Accorde l'autorisation de répertorier les domaines de pare-feu	Lecture	firewall-domain-list*		
ListFirewallRules	Accorde l'autorisation de répertorier les règles de pare-feu	List	dns-view*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGlobalResolvers	Accorde l'autorisation de répertorier les résolveurs globaux	List			
ListHostedZoneAssociations	Accorde l'autorisation de répertorier les associations de zones hébergées	List			
ListManagedFirewallDomainLists	Accorde l'autorisation de répertorier les listes de domaines de pare-feu gérés	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Écrire	access-source		
			access-token		
			dns-view		
			firewall-domain-list		
			global-resolver		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	access-source		
			access-token		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			dns-view		
			firewall-domain-list		
			global-resolver		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	access-source		
			access-token		
			dns-view		
			firewall-domain-list		
			global-resolver		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAccessSource	Autorise la mise à jour d'une source d'accès	Écrire	access-source*		
UpdateAccessToken	Autorise la mise à jour d'un jeton d'accès	Écrire	access-token*		
UpdateDNSView	Autorise la mise à jour d'une vue DNS	Écrire	dns-view*		
UpdateFirewallDomains	Accorde l'autorisation de mettre à jour les domaines du pare-feu	Écrire	firewall-domain-list*		
UpdateFirewallRule	Autorise la mise à jour d'une règle de pare-feu	Écrire			
UpdateGlobalResolver	Autorise la mise à jour d'un résolveur global	Écrire	global-resolver*		
UpdateHostedZoneAssociation	Accorde l'autorisation de mettre à jour une association de zone hébergée	Écrire			

Types de ressources définis par AWS Route53 Global Resolver

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
access-source	arn:${Partition}:route53globalresolver::${Account}:access-source/${Id}	aws:ResourceTag/${TagKey}
access-token	arn:${Partition}:route53globalresolver::${Account}:access-token/${Id}	aws:ResourceTag/${TagKey}
dns-view	arn:${Partition}:route53globalresolver::${Account}:dns-view/${Id}	aws:ResourceTag/${TagKey}
firewall-domain-list	arn:${Partition}:route53globalresolver::${Account}:firewall-domain-list/${Id}	aws:ResourceTag/${TagKey}
global-resolver	arn:${Partition}:route53globalresolver::${Account}:global-resolver/${Id}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Route53 Global Resolver

AWS Route53 Global Resolver définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS RTB Fabric

AWS RTB Fabric (préfixe de service :`rtbfabric`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS RTB Fabric
- Types de ressources définis par AWS RTB Fabric
- Clés de condition pour AWS RTB Fabric

Actions définies par AWS RTB Fabric

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptLink	Accorde l'autorisation d'accepter une invitation à un lien provenant d'une autre passerelle	Écrire	Link*		
CreateInboundExternalLink	Accorde l'autorisation de créer un lien externe entrant pour une passerelle de réponse	Écrire	ResponderGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLink	Autorise la création d'un nouveau lien entre les applications RTB	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutboundExternalLink	Accorde l'autorisation de créer un lien externe sortant permettant à une passerelle de demandeur de se connecter aux points de terminaison d'un répondeur public externe	Écrire	RequesterGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRequesterGateway	Accorde l'autorisation de créer une passerelle pour les demandeurs	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResponderGateway	Accorde l'autorisation de créer une passerelle de réponse	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteInboundExternalLink	Autorise la suppression d'un lien externe entrant	Écrire	InboundExternalLink*		
			ResponderGateway*		
DeleteLink	Autorise la suppression d'un lien entre les applications RTB	Écrire	Link*		
DeleteOutboundExternalLink	Autorise la suppression d'un lien externe sortant	Écrire	OutboundExternalLink*		
			RequesterGateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRequesterGateway	Accorde l'autorisation de supprimer une passerelle de demandeur	Écrire	RequesterGateway*		
DeleteResponderGateway	Autorise la suppression d'une passerelle de réponse	Écrire	ResponderGateway*		
GetInboundExternalLink	Accorde l'autorisation de récupérer des informations sur un lien externe entrant	Lecture	InboundExternalLink*		
			ResponderGateway*		
GetLink	Permet de récupérer des informations sur un lien entre des applications RTB	Lecture	Link*		
GetOutboundExternalLink	Accorde l'autorisation de récupérer des informations sur un lien externe sortant	Lecture	OutboundExternalLink*		
			RequesterGateway*		
GetRequesterGateway	Accorde l'autorisation de récupérer des informations sur une passerelle de demandeur	Lecture	RequesterGateway*		
GetResponderGateway	Accorde l'autorisation de récupérer des informations sur une passerelle de réponse	Lecture	ResponderGateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListLinks	Permet de répertorier les liens associés à une application RTB	List			
ListRequesterGateways	Accorde l'autorisation de répertorier les passerelles des demandeurs avec filtrage et pagination facultatifs	List			
ListResponderGateways	Accorde l'autorisation de répertorier les passerelles de réponse avec filtrage et pagination facultatifs	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	InboundExternalLink		
			Link		
			OutboundExternalLink		
			RequesterGateway		
			ResponderGateway		
RejectLink	Autorise le rejet d'une demande de lien entre des applications RTB	Écrire	Link*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'attribuer une ou plusieurs balises (paires clé-valeur) à la ressource spécifiée	Identification	InboundExternalLink		
			Link		
			OutboundExternalLink		
			RequesterGateway		
			ResponderGateway		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Identification	InboundExternalLink		
			Link		
			OutboundExternalLink		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Requester Gateway		
			Responder Gateway		
				aws:TagKeys	
UpdateLink	Accorde l'autorisation de mettre à jour les paramètres de configuration d'un lien existant	Écrire	Link*		
UpdateLinkModuleFlow	Autorise la mise à jour d'un flux de modules de liens	Écrire	Link*		
UpdateRequesterGateway	Autorise la mise à jour d'une passerelle de demandeur	Écrire	RequesterGateway*		
UpdateResponderGateway	Autorise la mise à jour d'une passerelle de réponse	Écrire	ResponderGateway*		

Types de ressources définis par AWS RTB Fabric

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
InboundExternalLink	`arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}/link/${LinkId}`	aws:ResourceTag/${TagKey} rtbfabric:InboundExternalLinkLinkId rtbfabric:ResponderGatewayGatewayId
Link	`arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}/link/${LinkId}`	aws:ResourceTag/${TagKey} rtbfabric:LinkLinkId rtbfabric:RequesterGatewayGatewayId rtbfabric:ResponderGatewayGatewayId
OutboundExternalLink	`arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}/link/${LinkId}`	aws:ResourceTag/${TagKey} rtbfabric:OutboundExternalLinkLinkId rtbfabric:RequesterGatewayGatewayId
RequesterGateway	`arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey} rtbfabric:RequesterGatewayGatewayId

Types de ressources	ARN	Clés de condition
Responder Gateway	`arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey} rtbfabric:ResponderGatewayGatewayId

Clés de condition pour AWS RTB Fabric

AWS RTB Fabric définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
rtbfabric:InboundExternalLinkGatewayId	Filtre l'accès par identifiant de passerelle compatible avec les formats rtb-gw-*	String

Clés de condition	Description	Type
rtbfabric:InboundExternalLinkLinkId	Filtre l'accès par identifiant InboundExternalLink LinkID de ressource	String
rtbfabric:LinkLinkId	Filtre l'accès par identifiant LinkID de la ressource Link	String
rtbfabric:OutboundExternalLinkLinkId	Filtre l'accès par identifiant OutboundExternalLink LinkID de ressource	String
rtbfabric:RequesterGatewayGatewayId	Filtre l'accès par identifiant de passerelle compatible avec les formats rtb-gw-*	String
rtbfabric:ResponderGatewayGatewayId	Filtre l'accès par identifiant de passerelle compatible avec les formats rtb-gw-*	String

Actions, ressources et clés de condition pour Amazon S3 Express

Amazon S3 Express (préfixe de service : `s3express`) fournit les ressources, les actions et les clés de contexte de condition propres au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon S3 Express

- Types de ressources définis par Amazon S3 Express
- Clés de condition pour Amazon S3 Express

Actions définies par Amazon S3 Express

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAccessPoint	Accorde l'autorisation de créer un nouveau point d'accès	Écriture	accesspoint*		
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
CreateBucket	Accorde l'autorisation de créer un nouveau compartiment	Écrire	bucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSession	Accorde l'autorisation de créer un jeton de session qui est utilisé pour APIs des objets tels que PutObject, GetObject, etc.	Écrire	bucket*		
			accesspoint	s3express:Permissions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:authType s3express:ResourceAccount s3express:SessionMode s3express:signatureAge s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 s3express:x-amz-server-side-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				encryption s3express:x-amz-server-side-encryption-aws-kms-key-id s3express:AllAccessRestrictedToLocalZoneGroup s3express:Permissions	
DeleteAccessPoint	Accorde l'autorisation de supprimer le point d'accès nommé dans l'URI	Écriture	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
DeleteAccessPointPolicy	Accorde l'autorisation de supprimer la politique sur un point d'accès spécifié	Gestion des autorisations	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
DeleteAccessPointScope	Accorde l'autorisation de supprimer la configuration de l'étendue sur un point d'accès spécifié	Gestion des autorisations	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
DeleteBucket	Accorde l'autorisation de supprimer le compartiment nommé dans l'URI	Écriture	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBucketPolicy	Accorde l'autorisation de supprimer la politique sur un compartiment spécifié	Gestion des autorisations	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
GetAccessPoint	Accorde l'autorisation de renvoyer des informations sur la configuration spécifiée.	Lecture	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
GetAccessPointPolicy	Accorde l'autorisation de renvoyer la politique de point d'accès associée au point d'accès spécifié	Lecture	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
GetAccessPointScope	Accorde l'autorisation de renvoyer la configuration de l'étendue associée au point d'accès spécifié	Lecture	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
GetBucketPolicy	Accorde l'autorisation de renvoyer la politique du compartiment spécifié	Lecture	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEncryptionConfiguration	Accorde l'autorisation de renvoyer la configuration de chiffrement par défaut pour un bucket d'annuaire	Lecture	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLifecycleConfiguration	Accorde l'autorisation de renvoyer les informations de configuration du cycle de vie définies dans un bucket d'annuaire	Lecture	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
GetMetricsConfiguration	Accorde l'autorisation d'obtenir la configuration des métriques d'un bucket d'annuaire	Lecture	bucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAccessPointsForDirectoryBuckets	Accorde l'autorisation de répertorier les points d'accès	List		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAllMyDirectoryBuckets	Octroie l'autorisation de répertorier tous les compartiments de répertoire appartenant à l'expéditeur authentifié de la demande.	List		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
ListTagsForResource	Accorde l'autorisation de répertorier tous les tags d'une ressource spécifiée	List	accesspoint bucket		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
PutAccessPointPolicy	Accorde l'autorisation d'associer une politique d'accès à un point d'accès spécifié	Gestion des autorisations	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
PutAccessPointScope	Accorde l'autorisation d'associer un point d'accès à une configuration d'étendue de point d'accès spécifiée	Gestion des autorisations	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				content-sha256	
PutBucketPolicy	Accorde l'autorisation d'ajouter ou de remplacer une politique de compartiment sur un compartiment	Gestion des autorisations	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutEncryptionConfiguration	Accorde l'autorisation de définir la configuration de chiffrement d'un compartiment de répertoires	Écrire	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutLifecycleConfiguration	Accorde l'autorisation de créer une nouvelle configuration de cycle de vie pour le compartiment de répertoire ou de remplacer une configuration de cycle de vie existante	Écrire	bucket*	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutMetricsConfiguration	Accorde l'autorisation de définir ou de mettre à jour une configuration de métriques pour les métriques de CloudWatch demande d'un bucket d'annuaire	Écrire	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
TagResource	Autorise la création d'un nouveau tag défini par l'utilisateur ou la mise à jour d'un tag existant	Identification	accesspoint		
			bucket		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises définies par l'utilisateur spécifiées d'une ressource S3	Identification	accesspoint		
			bucket		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 aws:TagKeys	

Types de ressources définis par Amazon S3 Express

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
bucket	`arn:${Partition}:s3express:${Region}:${Account}:bucket/${BucketName}`	aws:ResourceTag/${TagKey} s3express:BucketTag/${TagKey}
accesspoint	`arn:${Partition}:s3express:${Region}:${Account}:accesspoint/${AccessPointName}`	aws:ResourceTag/${TagKey} s3express:AccessPointTag/${TagKey}

Clés de condition pour Amazon S3 Express

Amazon S3 Express définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Clés de condition	Description	Type
s3express:AccessPointNetworkOrigin	Filtre l'accès en fonction de l'origine du réseau (Internet ou VPC)	String
s3express:AccessPointTag/${TagKey}	Filtre l'accès par paires clé-valeur de balise associées au point d'accès	String
s3express:AllAccessRestrictedToLocalZoneGroup	Filtre l'accès par groupe frontalier du réseau de zone AWS locale fourni dans cette clé de condition	String
s3express:BucketTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur associées au bucket	String
s3express:DataAccessPointAccount	Filtre l'accès en fonction de l'ID de AWS compte propriétaire du point d'accès	String
s3express:DataAccessPointArn	Filtre l'accès en fonction du point d'accès Amazon Resource Name (ARN)	ARN
s3express:LocationName	Filtre l'accès en fonction d'une zone de disponibilité ou d'un identifiant de zone locale spécifique	String
s3express:Permissions	Filtre l'accès en fonction de l'autorisation demandée par la configuration de l'étendue du point d'accès GetObject, par exemple PutObject	ArrayOfString
s3express:ResourceAccount	Filtre l'accès en fonction de l' Compte AWS ID du propriétaire de la ressource	String

Clés de condition	Description	Type
s3express:SessionMode	Filtre l'accès en fonction des autorisations demandées par CreateSession l'API, telles que ReadOnly et ReadWrite	String
s3express:TlsVersion	Filtre l'accès en fonction de la version TLS utilisée par le client	Numérique
s3express:authType	Filtre l'accès en fonction de la méthode d'authentification	Chaîne
s3express:signatureAge	Filtre l'accès en fonction de l'âge (en millisecondes) de la signature de la demande	Numérique
s3express:signatureversion	Filtre l'accès en fonction de la version de AWS signature utilisée sur la demande	String
s3express:x-amz-content-sha256	Filtre l'accès au contenu non signé dans votre compartiment	String
s3express:x-amz-server-side-encryption	Filtre l'accès en fonction du chiffrement côté serveur	String
s3express:x-amz-server-side-encryption-aws-kms-key-id	Filtre l'accès par clé gérée par le client AWS KMS pour le chiffrement côté serveur	ARN

Actions, ressources et clés de condition pour Amazon S3 Glacier

Amazon S3 Glacier (préfixe de service : `glacier`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon S3 Glacier
- Types de ressources définis par Amazon S3 Glacier
- Clés de condition pour Amazon S3 Glacier

Actions définies par Amazon S3 Glacier

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AbortMultipartUpload	Accorde l'autorisation d'interrompre un chargement partitionné identifié par l'ID de chargement	Écrire	vault*		
AbortVaultLock	Accorde l'autorisation d'interrompre le processus de verrouillage de coffre si celui-ci n'est pas dans l'état Verrouillé	Gestion des autorisations	vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddTagsToVault	Accorde l'autorisation d'ajouter des identifications spécifiées à un coffre	Identification	vault*		
CompleteMultipartUpload	Accorde l'autorisation de terminer un processus de chargement partitionné	Écrire	vault*		
CompleteVaultLock	Accorde l'autorisation de terminer le processus de verrouillage de coffre	Gestion des autorisations	vault*		
CreateVault	Accorde l'autorisation de créer un nouveau coffre avec le nom spécifié	Écrire	vault*		
DeleteArchive	Accorde l'autorisation de supprimer une archive d'un coffre	Écrire	vault*		
				glacier:ArchiveAgeInDays	
DeleteVault	Accorde l'autorisation de supprimer un coffre	Écrire	vault*		
DeleteVaultAccessPolicy	Accorde l'autorisation de supprimer la politique d'accès associée au coffre spécifié	Gestion des autorisations	vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteVaultNotifications	Accorde l'autorisation de supprimer la configuration de notification définie pour un coffre	Écrire	vault*		
DescribeJob	Accorde l'autorisation d'obtenir des informations sur une tâche précédemment initiée	Lecture	vault*		
DescribeVault	Accorde l'autorisation d'obtenir des informations sur un coffre	Lecture	vault*		
GetDataRetrievalPolicy	Accorde l'autorisation d'obtenir la politique d'extraction de données	Lecture			
GetJobOutput	Accorde l'autorisation de télécharger la sortie de la tâche spécifiée	Lecture	vault*		
GetVaultAccessPolicy	Accorde l'autorisation de récupérer la sous-ressource de politique d'accès définie sur le coffre	Lecture	vault*		
GetVaultLock	Accorde l'autorisation de récupérer les attributs de la sous-ressource de politique de verrouillage définie sur le coffre spécifié	Lecture	vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetVaultNotifications	Accorde l'autorisation de récupérer la sous-ressource de configuration des notifications définie sur le coffre	Lecture	vault*		
InitiateJob	Accorde l'autorisation de lancer une tâche du type spécifié	Écrire	vault*		
				glacier:ArchiveAgeInDays	
InitiateMultipartUpload	Accorde l'autorisation de démarrer un chargement partitionné	Écrire	vault*		
InitiateVaultLock	Accorde l'autorisation de démarrer le processus de verrouillage de coffre	Gestion des autorisations	vault*		
ListJobs	Accorde l'autorisation de répertorier les tâches relatives à un coffre qui sont en cours et les tâches récemment terminées	List	vault*		
ListMultipartUploads	Accorde l'autorisation de répertorier les chargements partitionnés en cours pour le coffre spécifié	List	vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListParts	Accorde l'autorisation de répertorier les parties d'une archive qui ont été chargées au cours d'un chargement partitionné spécifique	List	vault*		
ListProvisionedCapacity	Accorde l'autorisation de répertorier la capacité provisionnée pour la capacité spécifiée Compte AWS	List			
ListTagsForVault	Accorde l'autorisation de répertorier toutes les identifications attachées à un coffre	List	vault*		
ListVaults	Accorde l'autorisation de répertorier tous les coffres	List			
PurchaseProvisionedCapacity	Autorise l'achat d'une unité de capacité provisionnée pour un Compte AWS	Écrire			
RemoveTagsFromVault	Accorde l'autorisation de supprimer une ou plusieurs identifications dans la série d'identifications attachées à un coffre	Identification	vault*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetDataRetrievalPolicy	Accorde l'autorisation de définir, puis appliquer une politique de récupération de données dans la région spécifiée dans la requête PUT	Gestion des autorisations			
SetVaultAccessPolicy	Accorde l'autorisation de configurer une politique d'accès à un coffre ; cela remplacera toute politique existante	Gestion des autorisations	vault*		
SetVaultNotifications	Accorde l'autorisation de configurer les notifications du coffre	Écrire	vault*		
UploadArchive	Accorde l'autorisation de charger une archive dans un coffre	Écrire	vault*		
UploadMultipartPart	Accorde l'autorisation de charger une partie d'un archive	Écrire	vault*		

Types de ressources définis par Amazon S3 Glacier

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
vault	`arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}`	

Clés de condition pour Amazon S3 Glacier

Amazon S3 Glacier définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
glacier:ArchiveAgeInDays	Filtre l'accès par durée de stockage d'une archive dans le coffre, en jours	String
glacier:ResourceTag/	Filtre l'accès par identification définie par le client	String

Actions, ressources et clés de condition pour Amazon S3 Object Lambda

Amazon S3 Object Lambda (préfixe de service : `s3-object-lambda`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon S3 Object Lambda
- Types de ressources définis par Amazon S3 Object Lambda
- Clés de condition pour Amazon S3 Object Lambda

Actions définies par Amazon S3 Object Lambda

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AbortMultipartUpload	Accorde l'autorisation d'abandonner un téléchargement en plusieurs parties	Écriture	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:TlsVersion	
DeleteObject	Accorde l'autorisation de supprimer la version nulle d'un objet et d'insérer un marqueur de suppression, qui devient la version actuelle de l'objet	Écriture	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectTagging	Accorde l'autorisation d'utiliser la sous-ressource de balisage pour supprimer l'ensemble de identifications de l'objet spécifié	Balisage	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectVersion	Accorde l'autorisation de supprimer une version spécifique d'un objet	Écriture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
DeleteObjectVersionTagging	Accorde l'autorisation de supprimer l'ensemble de identifications pour une version spécifique de l'objet	Balisage	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObject	Accorde l'autorisation de récupérer des objets à partir d'Amazon S3	Lecture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectAcl	Accorde l'autorisation de renvoyer la liste de contrôle d'accès (ACL) d'un objet	Lecture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectLegalHold	Accorde l'autorisation d'obtenir le statut de blocage légal actuel d'un objet	Lecture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectRetention	Accorde l'autorisation de récupérer les paramètres de conservation d'un objet	Lecture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectTagging	Accorde l'autorisation de renvoyer le jeu de identifications d'un objet	Lecture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectVersion	Accorde l'autorisation de récupérer une version spécifique d'un objet	Lecture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionAcl	Accorde l'autorisation de renvoyer la liste de contrôle d'accès (ACL) d'une version d'objet spécifique	Read	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionTagging	Accorde l'autorisation de renvoyer le jeu de identifications pour une version spécifique de l'objet	Read	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
ListBucket	Accorde l'autorisation de répertorier tout ou partie des objets d'un compartiment Amazon S3 (jusqu'à 1 000)	Liste	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketMultipartUploads	Accorde l'autorisation de répertorier les téléchargements en plusieurs parties en cours	Liste	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketVersions	Accorde l'autorisation de répertorier les métadonnées sur toutes les versions d'objets d'un compartiment Amazon S3	Liste	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListMultipartUploadParts	Accorde l'autorisation de répertorier les articles qui ont été téléchargés pour un chargement en plusieurs parties spécifique	Liste	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObject	Accorde l'autorisation d'ajouter un objet à un compartiment	Écrire	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutObjectAcl	Accorde l'autorisation de définir les autorisations de liste de contrôle d'accès (ACL) pour des objets nouveaux ou existants dans un compartiment S3	Gestion des autorisations	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectLegalHold	Accorde l'autorisation d'appliquer une configuration de blocage légal à l'objet spécifié	Écriture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectRetention	Accorde l'autorisation de placer une configuration de conservation d'objet sur un objet	Écriture	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectTagging	Accorde l'autorisation de définir le jeu de identifications fourni sur un objet qui existe déjà dans un compartiment	Balisage	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutObjectVersionAcl	Accorde l'autorisation d'utiliser la sous-ressource acl pour définir les autorisations de liste de contrôle d'accès (ACL) pour un objet qui existe déjà dans un compartiment	Gestion des autorisations	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
PutObjectVersionTagging	Accorde l'autorisation de définir le jeu de identifications fourni pour une version spécifique d'un objet	Balisage	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
RestoreObject	Accorde l'autorisation de restaurer une copie archivée d'un objet dans Amazon S3	Écrire	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
WriteGetObjectResponse	Accorde l'autorisation de fournir des données pour les GetObject demandes envoyées à S3 Object Lambda	Écrire	objectlambdaaccesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Types de ressources définis par Amazon S3 Object Lambda

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
objectlambdaaccesspoint	`arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}`	

Clés de condition pour Amazon S3 Object Lambda

Amazon S3 Object Lambda définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
s3-object-lambda:TlsVersion	Filtre l'accès en fonction de la version TLS utilisée par le client	Numérique
s3-object-lambda:authType	Filtre l'accès en fonction de la méthode d'authentification	Chaîne
s3-object-lambda:signatureAge	Filtre l'accès en fonction de l'âge (en millisecondes) de la signature de la demande	Numérique
s3-object-lambda:versionid	Filtre l'accès en fonction d'une version d'objet spécifique	Chaîne

Actions, ressources et clés de condition pour Amazon S3 on Outposts

Amazon S3 on Outposts (préfixe de service : `s3-outposts`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon S3 on Outposts
- Types de ressources définis par Amazon S3 on Outposts
- Clés de condition pour Amazon S3 on Outposts

Actions définies par Amazon S3 on Outposts

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AbortMultipartUpload	Accorde l'autorisation d'abandonner un téléchargement en plusieurs parties	Écriture	object*		
				s3-outposts:DataAc	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				cessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:x-amz-content-sha256	
CreateAccessPoint	Accorde l'autorisation de créer un nouveau point d'accès	Écriture	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:x-amz-content-sha256	
CreateBucket	Accorde l'autorisation de créer un nouveau compartiment	Écriture	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEndpoint	Octroie l'autorisation de créer un nouveau point de terminaison	Écriture	endpoint*		
DeleteAccessPoint	Accorde l'autorisation de supprimer le point d'accès nommé dans l'URI	Écriture	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:x-amz-content-sha256	
DeleteAccessPointPolicy	Accorde l'autorisation de supprimer la politique sur un point d'accès spécifié	Gestion des autorisations	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:x-amz-content-sha256	
DeleteBucket	Accorde l'autorisation de supprimer le compartiment nommé dans l'URI	Écriture	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteBucketPolicy	Accorde l'autorisation de supprimer la politique sur un compartiment spécifié	Gestion des autorisations	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteEndpoint	Accorde l'autorisation de supprimer le point de terminaison nommé dans l'URI	Écriture	endpoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteObject	Accorde l'autorisation de supprimer la version nulle d'un objet et d'insérer un marqueur de suppression, qui devient la version actuelle de l'objet	Écriture	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteObjectTagging	Accorde l'autorisation d'utiliser la sous-ressource de balisage pour supprimer l'ensemble de identifications de l'objet spécifié	Balisage	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteObjectVersion	Accorde l'autorisation de supprimer une version spécifique d'un objet	Écriture	object*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteObjectVersionTagging	Accorde l'autorisation de supprimer l'ensemble de identifications pour une version spécifique de l'objet	Identification	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccessPoint	Accorde l'autorisation de renvoyer des informations sur la configuration spécifiée.	Lecture		s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:x-amz-content-sha256	
GetAccessPointPolicy	Accorde l'autorisation de renvoyer la politique de point d'accès associée au point d'accès spécifié	Lecture	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:x-amz-content-sha256	
GetBucket	Accorde l'autorisation de renvoyer la configuration de compartiment associée à un compartiment Amazon S3	Lecture	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBucketPolicy	Accorde l'autorisation de renvoyer la politique du compartiment spécifié	Lecture	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBucketTagging	Accorde l'autorisation de renvoyer le jeu de identifications associé à un compartiment Amazon S3	Lecture	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetBucketVersioning	Accorde l'autorisation de renvoyer l'état de contrôle de version d'un compartiment Amazon S3	Lecture	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLifecycleConfiguration	Accorde l'autorisation de renvoyer les informations de configuration du cycle de vie définies sur un compartiment Amazon S3	Lecture	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObject	Accorde l'autorisation de récupérer des objets à partir d'Amazon S3	Lecture	object*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectTagging	Accorde l'autorisation de renvoyer le jeu de identifications d'un objet	Lecture	object*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObjectVersion	Accorde l'autorisation de récupérer une version spécifique d'un objet	Lecture	object*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetObjectVersionForReplication	Accorde l'autorisation de répliquer à la fois des objets non chiffrés et des objets chiffrés avec SSE-KMS	Lecture	object*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetObjectVersionTagging	Accorde l'autorisation de renvoyer le jeu de identifications pour une version spécifique de l'objet	Read	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetReplicationConfiguration	Accorde l'autorisation d'obtenir les informations de configuration de réplication définies sur un compartiment Amazon S3	Lecture	bucket*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAccessPoints	Accorde l'autorisation de répertorier les points d'accès	Liste		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucket	Accorde l'autorisation de répertorier tout ou partie des objets d'un compartiment Amazon S3 (jusqu'à 1 000)	Liste	accesspoint* bucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outposts:max-keys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucketMultipartUploads	Accorde l'autorisation de répertorier les téléchargements en plusieurs parties en cours	Liste	accesspoint* bucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBucketVersions	Accorde l'autorisation de répertorier les métadonnées sur toutes les versions d'objets d'un compartiment Amazon S3	List	bucket*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:max-keys s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListEndpoints	Accorde l'autorisation de répertorier les points de terminaison	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMultipartUploadParts	Accorde l'autorisation de répertorier les articles qui ont été téléchargés pour un chargement en plusieurs parties spécifique	List	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:signatureversion s3-outposts:x-amz-content-sha256	
ListOutpostsWithS3	Octroie l'autorisation de répertorier les outposts dotés d'une capacité S3	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRegionalBuckets	Accorde l'autorisation de répertorier tous les compartiments appartenant à l'expéditeur authentifié de la demande	List		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListSharedEndpoints	Accorde l'autorisation de répertorier les points de terminaison partagés	List			
PutAccessPointPolicy	Accorde l'autorisation d'associer une politique d'accès à un point d'accès spécifié	Gestion des autorisations	accesspoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ureversion s3-outposts:x-amz-content-sha256	
PutBucketPolicy	Accorde l'autorisation d'ajouter ou de remplacer une politique de compartiment sur un compartiment	Gestion des autorisations	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutBucketTagging	Accorde l'autorisation d'ajouter un jeu de balises à un compartiment Amazon S3 existant	Balisage	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutBucketVersioning	Accorde l'autorisation de définir l'état de contrôle de version d'un compartiment Amazon S3 existant	Écrire	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutLifecycleConfiguration	Accorde l'autorisation de créer une nouvelle configuration de cycle de vie pour le compartiment ou de remplacer une configuration de cycle de vie existante	Écriture	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
PutObject	Accorde l'autorisation d'ajouter un objet à un compartiment	Écriture	object*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:RequestObjectTag/<key> s3-outposts:RequestObjectTagKeys s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-copy-source s3-outpos	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ts:x-amz-metadata-directive s3-outposts:x-amz-server-side-encryption s3-outposts:x-amz-storage-class	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutObjectAcl	Accorde l'autorisation de définir les autorisations de liste de contrôle d'accès (ACL) pour un objet qui existe déjà dans un compartiment	Gestion des autorisations	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-storage-class	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutObjectTagging	Accorde l'autorisation de définir le jeu de balises fourni sur un objet qui existe déjà dans un compartiment	Identification	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key>	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutObjectVersionTagging	Accorde l'autorisation de définir le jeu de identifications fourni pour une version spécifique d'un objet	Balisage	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key>	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3-outposts:RequestObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutReplicationConfiguration	Accorde l'autorisation de créer une nouvelle configuration de réplication ou de remplacer une configuration existante	Écrire	bucket*		iam:PassRole
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Replicate Delete	Accorde l'autorisation de répliquer les marqueurs de suppression vers le compartiment de destination	Écriture	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Replicate Object	Accorde l'autorisation de répliquer des objets et des identifications d'objet vers le compartiment de destination	Écriture	object*	s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-server-side-encryption	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Replicate Tags	Accorde l'autorisation de répliquer les identifications d'objet vers le compartiment de destination	Identification	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Types de ressources définis par Amazon S3 on Outposts

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
accesspoint	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/accesspoint/${AccessPointName}`	
bucket	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}`	
endpoint	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/endpoint/${EndpointId}`	
object	`arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}/object/${ObjectName}`	

Clés de condition pour Amazon S3 on Outposts

Amazon S3 on Outposts définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
s3-outposts:Access	Filtre l'accès en fonction de l'origine du réseau (Internet ou VPC)	String

Clés de condition	Description	Type
PointNetworkOrigin		
s3-outposts:DataAccessPointAccount	Filtre l'accès en fonction de l'ID de AWS compte propriétaire du point d'accès	String
s3-outposts:DataAccessPointArn	Filtre l'accès en fonction du point d'accès Amazon Resource Name (ARN)	ARN
s3-outposts:ExistingObjectTag/<key>	Filtre l'accès en exigeant qu'une balise d'objet existante ait une clé et une valeur de balise spécifiques	Chaîne
s3-outposts:RequestObjectTag/<key>	Filtre l'accès en limitant les clés et valeurs de balise autorisées sur les objets	Chaîne
s3-outposts:RequestObjectTagKeys	Filtre l'accès en limitant les clés de balise autorisées sur les objets	Chaîne
s3-outposts:authType	Filtre l'accès en limitant les demandes entrantes à une méthode d'authentification spécifique	Chaîne
s3-outposts:delimiter	Filtre l'accès en exigeant le paramètre de délimiteur	String
s3-outposts:max-keys	Filtre l'accès en limitant le nombre maximum de clés renvoyées dans une ListBucket demande	Numérique
s3-outposts:prefix	Filtre l'accès en fonction du préfixe de nom de clé	Chaîne

Clés de condition	Description	Type
s3-outposts:signatureAge	Filtre l'accès en identifiant la durée, en millisecondes, pendant laquelle une signature est valide dans une demande authentifiée	Numérique
s3-outposts:signatureversion	Filtre l'accès en identifiant la version de AWS Signature prise en charge pour les demandes authentifiées	String
s3-outposts:versionid	Filtre l'accès en fonction d'une version d'objet spécifique	String
s3-outposts:x-amz-acl	Filtre l'accès en exigeant l' x-amz-aclen-tête avec une ACL prédéfinie spécifique dans une demande	String
s3-outposts:x-amz-content-sha256	Filtre l'accès en refusant les contenus non signés dans votre compartiment	Chaîne
s3-outposts:x-amz-copy-source	Filtre l'accès en limitant la source de copie à un compartiment, un préfixe ou un objet spécifique	Chaîne
s3-outposts:x-amz-metadata-directive	Filtre l'accès en activant l'application du comportement des métadonnées d'objet (COPY ou REPLACE) lorsque des objets sont copiés	Chaîne
s3-outposts:x-amz-server-side-encryption	Filtre l'accès en exigeant un chiffrement côté serveur	Chaîne
s3-outposts:x-amz-storage-class	Filtre l'accès en fonction de la classe de stockage.	String

Actions, ressources et clés de condition pour les tables Amazon S3

Amazon S3 Tables (préfixe de service :`s3tables`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les tables Amazon S3
- Types de ressources définis par les tables Amazon S3
- Clés de condition pour les tables Amazon S3

Actions définies par les tables Amazon S3

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateNamespace	Accorde l'autorisation de créer un espace de noms	Écrire	TableBucket*		
CreateTable	Accorde l'autorisation de créer une table.	Écrire	TableBucket*		
				s3tables:namespace	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3tables:SSEAlgorithm s3tables:KMSKeyAr s3tables:TableBucketTag/${TagKey} aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTableBucket	Accorde l'autorisation de créer un bucket de tables	Écrire	TableBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3tables:SSEAlgorithm s3tables:KMSKeyAr s3tables:TableBucketTag/${TagKey} aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteNamespace	Accorde l'autorisation de supprimer un espace de noms	Écrire	TableBucket*		
				s3tables:namespace	
DeleteTable	Accorde l'autorisation de supprimer une table.	Écrire	Table*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3tables:namespace s3tables:tableName	
DeleteTableBucket	Autorise la suppression d'un bucket de table	Écrire	TableBucket*		
DeleteTableBucketEncryption	Accorde l'autorisation de supprimer la configuration de chiffrement sur un bucket de table	Écrire	TableBucket*		
DeleteTableBucketMetricsConfiguration	Accorde l'autorisation de supprimer une configuration de métriques dans un bucket de table	Écrire	TableBucket*		
DeleteTableBucketPolicy	Accorde l'autorisation de supprimer une politique sur un bucket de tables	Gestion des autorisations	TableBucket*		
DeleteTableBucketReplication	Accorde l'autorisation de supprimer la configuration de réplication des compartiments de tables sur un compartiment	Écrire	TableBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTableLePolicy	Accorde l'autorisation de supprimer une politique sur une table	Gestion des autorisations	Table*		
				s3tables:namespace s3tables:tableName	
DeleteTableReplication	Accorde l'autorisation de supprimer la configuration de réplication de table sur une table	Écrire	Table*		
				s3tables:namespace s3tables:tableName	
GetNamespace	Accorde l'autorisation d'obtenir un espace de noms	Lecture	TableBucket*		
				s3tables:namespace	
GetTable	Accorde l'autorisation de récupérer une table.	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableBucket	Accorde l'autorisation de récupérer un bucket de tables	Lecture	TableBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTableBucketEncryption	Accorde l'autorisation de récupérer la configuration de chiffrement sur un bucket de table	Lecture	TableBucket*		
GetTableBucketMaintenanceConfiguration	Accorde l'autorisation de récupérer une configuration de maintenance sur un bucket de table	Lecture	TableBucket*		
GetTableBucketMetricsConfiguration	Accorde l'autorisation de récupérer une configuration de métriques sur un bucket	Lecture	TableBucket*		
GetTableBucketPolicy	Accorde l'autorisation de récupérer une politique sur un bucket de tables	Lecture	TableBucket*		
GetTableBucketReplication	Accorde l'autorisation de récupérer la configuration de réplication d'un compartiment de tables sur un compartiment	Lecture	TableBucket*		
GetTableBucketStorageClass	Accorde l'autorisation de récupérer la configuration de classe de stockage pour un bucket de table	Lecture	TableBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTableData [autorisation uniquement]	Accorde l'autorisation de lire les métadonnées et les objets de données à partir d'un point de terminaison de stockage de tables à l'aide de S3 APIs	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableEncryption	Accorde l'autorisation de récupérer la configuration de chiffrement sur une table	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMaintenanceConfiguration	Accorde l'autorisation de récupérer une configuration de maintenance sur une table	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableMaintenanceJobStatus	Accorde l'autorisation de récupérer le statut des tâches de maintenance sur une table	Lecture	Table*		
				s3tables:namespace s3tables:tableName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTableMetadataLocation	Accorde l'autorisation de récupérer l'emplacement des métadonnées d'une table	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTablePolicy	Accorde l'autorisation de récupérer une politique sur une table	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableRecordExpirationConfiguration	Accorde l'autorisation de récupérer une configuration de maintenance de table sur une table système	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableRecordExpirationJobStatus	Accorde l'autorisation de récupérer l'état des tâches d'expiration des enregistrements de table sur une table système	Lecture	Table*		
				s3tables:namespace s3tables:tableName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTableReplication	Accorde l'autorisation de récupérer une configuration de réplication de table sur une table	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableReplicationStatus	Accorde l'autorisation de récupérer le statut de réplication d'une table sur une table	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
GetTableStorageClass	Accorde l'autorisation de récupérer la configuration de classe de stockage pour une table spécifique	Lecture	Table*		
				s3tables:namespace s3tables:tableName	
ListNamespaces	Accorde l'autorisation de répertorier les espaces de noms	List	TableBucket*		
ListTableBuckets	Accorde l'autorisation de répertorier les compartiments de table	List			
ListTables	Accorde l'autorisation de répertorier les tables	List	TableBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				s3tables:namespace	
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource S3 Tables	List	Table		
			TableBucket		
				aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}	
PutTableBucketEncryption	Accorde l'autorisation de placer ou de remplacer la configuration de chiffrement sur un bucket de table	Écrire	TableBucket*		
				s3tables:KMSKeyAr s3tables:SSEAlgorithm	
PutTableBucketMaintenanceConfiguration	Accorde l'autorisation de placer une configuration de maintenance sur un bucket de table	Écrire	TableBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutTableBucketMetricsConfiguration	Accorde l'autorisation de créer ou de remplacer une configuration de métriques sur un bucket de tables	Écrire	TableBucket*		
PutTableBucketPolicy	Accorde l'autorisation de créer ou de remplacer une politique sur un bucket de tables	Gestion des autorisations	TableBucket*		
PutTableBucketReplication	Accorde l'autorisation de placer la configuration de réplication des compartiments de table sur un compartiment	Écrire	TableBucket*		
PutTableBucketStorageClass	Accorde l'autorisation de définir ou de mettre à jour la configuration de classe de stockage pour un bucket de tables	Écrire	TableBucket*		
				s3tables:StorageClass	
PutTableData [autorisation uniquement]	Accorde l'autorisation d'écrire des métadonnées et des objets de données sur un point de terminaison de stockage de tables à l'aide de S3 APIs	Écrire	Table*		
				s3tables:namespace s3tables:tableName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutTableEncryption [autorisation uniquement]	Accorde l'autorisation de placer la configuration de chiffrement sur une table	Écrire	Table*		
				s3tables:namespace s3tables:SSEAlgorithm s3tables:KMSKeyAr	
PutTableMaintenanceConfiguration	Accorde l'autorisation de mettre une configuration de maintenance sur une table	Écrire	Table*		
				s3tables:namespace s3tables:tableName	
PutTablePolicy	Accorde l'autorisation de créer ou de remplacer une politique sur une table	Gestion des autorisations	Table*		
				s3tables:namespace s3tables:tableName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutTableRecordExpirationConfiguration	Accorde l'autorisation de placer une configuration d'expiration d'enregistrement de table sur une table système	Écrire	Table*		
				s3tables:namespace s3tables:tableName	
PutTableReplication	Accorde l'autorisation de placer la configuration de réplication de table sur une table	Écrire	Table*		
				s3tables:namespace s3tables:tableName	
PutTableStorageClass	Accorde l'autorisation de définir ou de mettre à jour la configuration de classe de stockage pour une table	Écrire	Table*		
				s3tables:namespace s3tables:tableName s3tables:StorageClass	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RenameTable	Accorde l'autorisation de renommer une table ou de déplacer une table entre des espaces de noms	Écrire	Table*		
				s3tables:namespace s3tables:tableName	
TagResource	Accorde l'autorisation de baliser une ressource S3 Tables	Identification	Table		
			TableBucket		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer le balisage d'une ressource S3 Tables	Identification	Table		
			TableBucket		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}	
UpdateTableMetadataLocation	Accorde l'autorisation de mettre à jour l'emplacement des métadonnées d'une table	Écrire	Table*		
				s3tables:namespace s3tables:tableName	

Types de ressources définis par les tables Amazon S3

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
TableBucket	`arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}`	aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}
Table	`arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}/table/${TableID}`	aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey} s3tables:namespace s3tables:tableName

Clés de condition pour les tables Amazon S3

Amazon S3 Tables définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
s3tables:KMSKeyArn	Filtre l'accès par l'ARN de la clé AWS KMS utilisée pour chiffrer une table	ARN
s3tables:SSEAlgorithm	Filtre l'accès par l'algorithme de chiffrement côté serveur utilisé pour chiffrer une table	String
s3tables:StorageClass	Filtre l'accès en fonction de la classe de stockage qui peut être définie sur les tables situées dans un bucket de tables	String
s3tables:TableBucketTag/${TagKey}	Filtre l'accès en fonction des balises associées au compartiment de table	String
s3tables:namespace	Filtre l'accès en fonction des espaces de noms créés dans le compartiment de table	String
s3tables:tableName	Filtre l'accès en fonction du nom des tables dans le compartiment de tables	String

Actions, ressources et clés de condition pour les vecteurs Amazon S3

Amazon S3 Vectors (préfixe de service :`s3vectors`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon S3 Vectors
- Types de ressources définis par Amazon S3 Vectors
- Clés de condition pour les vecteurs Amazon S3

Actions définies par Amazon S3 Vectors

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIndex	Accorde l'autorisation de créer un nouvel index vectoriel dans un compartiment vectoriel spécifié	Écrire	Index*		
				s3vectors:sseType s3vectors:kmsKeyArn aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBu	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				cketTag/${TagKey}	
CreateVectorBucket	Accorde l'autorisation de créer un nouveau bucket vectoriel	Écrire	VectorBucket*		
				s3vectors:sseType s3vectors:kmsKeyArn aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteIndex	Accorde l'autorisation de supprimer un index vectoriel spécifié	Écrire	Index*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
DeleteVectorBucket	Accorde l'autorisation de supprimer un compartiment vectoriel spécifié	Écrire	VectorBucket*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
DeleteVectorBucketPolicy	Accorde l'autorisation de supprimer la politique de ressources IAM d'un bucket vectoriel spécifié	Gestion des autorisations	VectorBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
DeleteVectors	Accorde l'autorisation de supprimer un lot de vecteurs d'un index vectoriel spécifié	Écrire	Index*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetIndex	Accorde l'autorisation d'obtenir les attributs d'un index vectoriel spécifié	Lecture	Index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetVectorBucket	Accorde l'autorisation d'obtenir les attributs d'un bucket vectoriel spécifié	Lecture	VectorBucket*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetVectorBucketPolicy	Accorde l'autorisation d'obtenir la politique de ressources IAM pour un bucket vectoriel spécifique	Lecture	VectorBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetVectors	Permet d'obtenir un lot de vecteurs à l'aide de leurs clés vectorielles	Lecture	Index*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
ListIndexes	Accorde l'autorisation d'obtenir une liste paginée de tous les index d'un compartiment vectoriel spécifié	List	VectorBucket*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour la ressource S3Vector spécifiée	List	Index		
			VectorBucket		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
ListVectorBuckets	Permet d'obtenir une liste paginée de tous les compartiments vectoriels du compte	List			
ListVectors	Accorde l'autorisation d'obtenir une liste paginée de tous les vecteurs dans un index vectoriel spécifié	List	Index*		s3vectors:GetVectors

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
PutVectorBucketPolicy	Accorde l'autorisation d'ajouter une politique de ressources IAM à un compartiment vectoriel spécifié	Gestion des autorisations	VectorBucket*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
PutVectors	Accorde l'autorisation d'ajouter un lot de vecteurs à un index vectoriel spécifié	Écrire	Index*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
QueryVectors	Accorde l'autorisation de trouver les voisins les plus proches approximatifs dans un index de vecteur de recherche spécifié pour un vecteur de requête donné	Lecture	Index*		s3vectors:GetVectors
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser une ressource S3Vector	Identification	Index		
			VectorBucket		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
UntagResource	Accorde l'autorisation de détaguer une ressource S3Vector	Identification	Index VectorBucket		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	

Types de ressources définis par Amazon S3 Vectors

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Index	`arn:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}/index/${IndexName}`	aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}

Types de ressources	ARN	Clés de condition
VectorBucket	`arn:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}`	aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}

Clés de condition pour les vecteurs Amazon S3

Amazon S3 Vectors définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
s3vectors:VectorBucketTag/${TagKey}	Filtre l'accès en fonction des balises associées au bucket vectoriel	String
s3vectors:kmsKeyArn	Filtre l'accès par l'ARN de la clé AWS KMS pour la clé utilisée pour chiffrer un bucket vectoriel	ARN

Clés de condition	Description	Type
s3vectors:sseType	Filtre l'accès par type de chiffrement côté serveur	String

Actions, ressources et clés de condition pour Amazon SageMaker Data Science Assistant

Amazon SageMaker Data Science Assistant (préfixe de service :`sagemaker-data-science-assistant`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'assistant scientifique SageMaker des données Amazon
- Types de ressources définis par l'assistant scientifique SageMaker des données Amazon
- Clés de condition pour Amazon SageMaker Data Science Assistant

Actions définies par l'assistant scientifique SageMaker des données Amazon

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendConversation [autorisation uniquement]	Autorise le lancement d'une conversation avec un assistant en science SageMaker des données	Écrire			

Types de ressources définis par l'assistant scientifique SageMaker des données Amazon

Amazon SageMaker Data Science Assistant ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon SageMaker Data Science Assistant, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Amazon SageMaker Data Science Assistant

SageMakerDataScienceAssistant ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les fonctionnalités SageMaker géospatiales d'Amazon

Les fonctionnalités SageMaker géospatiales d'Amazon (préfixe de service :`sagemaker-geospatial`) fournissent les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les fonctionnalités SageMaker géospatiales d'Amazon
- Types de ressources définis par les fonctionnalités SageMaker géospatiales d'Amazon
- Clés de condition pour les fonctionnalités SageMaker géospatiales d'Amazon

Actions définies par les fonctionnalités SageMaker géospatiales d'Amazon

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEarthObservationJob	Autorise l' DeleteEarthObservationJob opération qui supprime une tâche d'observation de la Terre existante	Écrire	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
DeleteVectorEnrichmentJob	Autorise l' DeleteVectorEnrichmentJob opération qui supprime une tâche d'enrichissement vectoriel existante	Écrire	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExportEarthObservationJob	Accorde l'autorisation de copier les résultats d'une tâche d'observation de la terre vers un emplacement S3	Écrire	EarthObservationJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
ExportVectorEnrichmentJob	Accorde l'autorisation de copier les résultats d'un VectorEnrichmentJob vers un emplacement S3	Écrire	VectorEnrichmentJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
GetEarthObservationJob	Accorde l'autorisation de renvoyer des informations sur la tâche d'observation de la terre	Lecture	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
GetRasterDataCollection	Accorde l'autorisation de renvoyer des informations sur la collecte de données matricielles	Lecture	RasterDataCollection*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTile	Accorde l'autorisation d'obtenir la tuile d'une tâche d'observation de la terre	Lecture	EarthObservationJob*		iam:PassRole
GetVectorEnrichmentJob	Accorde l'autorisation de renvoyer des informations sur la tâche d'enrichissement vectoriel	Lecture	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ListEarthObservationJobs	Accorde l'autorisation de renvoyer un tableau des tâches d'observation de la terre associé au compte actuel	List			
ListRasterDataCollections	Accorde l'autorisation de renvoyer un tableau des collections de données matricielles associées au nom de modèle donné	List			
ListTagsForResource	Autorise l'utilisation des balises de liste pour une SageMaker ressource géospatiale	List	EarthObservationJob		
			RasterDataCollection		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			VectorEnrichmentJob		
				aws:ResourceTag/${TagKey}	
ListVectorEnrichmentJobs	Accorde l'autorisation de renvoyer un tableau des tâches d'enrichissement vectoriel associées au compte actuel	List			
SearchRasterDataCollection	Accorde l'autorisation d'interroger les collections de données matricielles	Lecture			
StartEarthObservationJob	Autorise l' StartEarthObservationJob opération qui lance une nouvelle tâche d'observation de la Terre sur votre compte	Écrire	EarthObservationJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartVectorEnrichmentJob	Autorise l' StartVectorEnrichmentJob opération qui lance une nouvelle tâche d'enrichissement vectoriel sur votre compte	Écrire	VectorEnrichmentJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopEarthObservationJob	Autorise l' StopEarthObservationJob opération qui met fin à un travail d'observation de la Terre existant	Écrire	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
StopVectorEnrichmentJob	Autorise l' StopVectorEnrichmentJob opération qui arrête une tâche d'enrichissement vectoriel existante	Écrire	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser une SageMaker ressource géospatiale	Identification	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Autorise le débalisage d'une ressource SageMaker géospatiale	Identification	EarthObservationJob		
			RasterDataCollection		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			VectorEnrichmentJob		
				aws:TagKeys	

Types de ressources définis par les fonctionnalités SageMaker géospatiales d'Amazon

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
EarthObservationJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:earth-observation-job/${JobID}`	aws:ResourceTag/${TagKey}
RasterDataCollection	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:raster-data-collection/${CollectionID}`	aws:ResourceTag/${TagKey}
VectorEnrichmentJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:vector-enrichment-job/${JobID}`	aws:ResourceTag/${TagKey}

Clés de condition pour les fonctionnalités SageMaker géospatiales d'Amazon

Les fonctionnalités SageMaker géospatiales d'Amazon définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon SageMaker Unified Studio MCP

Amazon SageMaker Unified Studio MCP (préfixe de service :`sagemaker-unified-studio-mcp`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon SageMaker Unified Studio MCP

- Types de ressources définis par Amazon SageMaker Unified Studio MCP
- Clés de condition pour Amazon SageMaker Unified Studio MCP

Actions définies par Amazon SageMaker Unified Studio MCP

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CallPrivilegedTool [autorisation uniquement]	Accorde l'autorisation d'appeler des outils privilégiés dans le service MCP	Écrire			
CallReadOnlyTool [autorisation uniquement]	Accorde l'autorisation d'appeler des outils en lecture seule dans le service MCP	Lecture			
InvokeMcp [autorisation uniquement]	Autorise l'utilisation du service MCP	Lecture			

Types de ressources définis par Amazon SageMaker Unified Studio MCP

Amazon SageMaker Unified Studio MCP ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon SageMaker Unified Studio MCP, spécifiez-le `"Resource": "*"` dans votre politique.

Clés de condition pour Amazon SageMaker Unified Studio MCP

SageMaker Unified Studio MCP ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon SageMaker avec MLflow

Amazon SageMaker with MLflow (préfixe de service :`sagemaker-mlflow`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon SageMaker avec MLflow
- Types de ressources définis par Amazon SageMaker avec MLflow
- Clés de condition pour Amazon SageMaker avec MLflow

Actions définies par Amazon SageMaker avec MLflow

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AccessUI	Accorde l'autorisation d'accéder à l' MLflow interface utilisateur	Lecture			
CreateExperiment	Accorde l'autorisation de créer une MLflow expérience	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
CreateModelVersion	Accorde l'autorisation de créer une nouvelle version du modèle	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
CreateRegisteredModel	Autorise la création d'un modèle enregistré	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
CreateRun	Autorise la création d'une nouvelle série dans le cadre d'une expérience	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteExperiment	Accorde l'autorisation de marquer une MLflow expérience pour suppression	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteLoggedModel	Accorde l'autorisation de supprimer un modèle connecté MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteLoggedModelTag	Accorde l'autorisation de supprimer un tag pour un modèle connecté MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteModelVersion	Autorise la suppression d'une version de modèle	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteModelVersionTag	Autorise la suppression d'une balise de version du modèle	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteRegisteredModel	Autorise la suppression d'un modèle enregistré	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteRegisteredModelAlias	Autorise la suppression d'un alias de modèle enregistré	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteRegisteredModelTag	Autorise la suppression d'une étiquette de modèle enregistrée	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteRun	Accorde l'autorisation de marquer une course pour suppression	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteTag	Accorde l'autorisation de supprimer un tag lors d'une course	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteTraceTag	Accorde l'autorisation de supprimer une balise de trace dans MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTraces	Accorde l'autorisation de supprimer des traces dans MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
EndTrace	Accorde l'autorisation de mettre fin à une trace dans MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
FinalizeLoggedModel	Accorde l'autorisation de définir le statut d'un modèle connecté MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetDownloadURIForModelVersionArtifacts	Accorde l'autorisation d'obtenir une URI pour télécharger des artefacts de modèle pour une version de modèle spécifique	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetExperiment	Accorde l'autorisation d'obtenir des métadonnées pour une MLflow expérience	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetExperimentByName	Accorde l'autorisation d'obtenir les métadonnées d'une MLflow expérience par son nom	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetLatestModelVersions	Accorde l'autorisation d'obtenir les dernières versions du modèle	List	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLoggedModel	Accorde l'autorisation d'accéder à un modèle connecté MLflow	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetMetricHistory	Accorde l'autorisation d'obtenir une liste de toutes les valeurs de la métrique spécifiée pour une exécution donnée	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetModelVersion	Accorde l'autorisation d'obtenir une version de modèle par nom de modèle et par version	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetModelVersionByAlias	Accorde l'autorisation d'obtenir la version du modèle par alias dans MLflow	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetRegisteredModel	Donne l'autorisation d'obtenir un modèle enregistré	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetRun	Accorde l'autorisation d'obtenir des métadonnées, des métriques, des paramètres et des balises pour une exécution	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetTraceInfo	Accorde l'autorisation d'obtenir des informations sur une trace dans MLflow	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListArtifacts	Accorde l'autorisation de répertorier les artefacts pour une exécution	List	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
ListLoggedModelArtifacts	Accorde l'autorisation de répertorier les artefacts d'un modèle connecté MLflow	List	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogBatch	Autorise l'enregistrement d'un lot de métriques, de paramètres et de balises pour une exécution	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogInputs	Accorde l'autorisation de consigner les entrées pour une exécution	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogLoggedModelParams	Accorde l'autorisation de consigner les paramètres d'un modèle connecté MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogMetric	Accorde l'autorisation d'enregistrer une métrique pour une exécution	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogModel	Accorde l'autorisation de consigner le modèle associé à une exécution	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
LogOutputs	Accorde l'autorisation de consigner les sorties, telles que les modèles, pour une exécution MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogParam	Accorde l'autorisation d'enregistrer un paramètre suivi pendant une exécution	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
RenameRegisteredModel	Autorise le changement de nom d'un modèle enregistré	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
RestoreExperiment	Autorise la restauration d'une expérience marquée pour suppression	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
RestoreRun	Accorde l'autorisation de restaurer une course supprimée	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchExperiments	Donne l'autorisation de rechercher MLflow des expériences	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchLoggedModels	Accorde l'autorisation de rechercher des modèles connectés MLflow	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchModelVersions	Autorise la recherche d'une version de modèle	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchRegisteredModels	Autorise la recherche de modèles enregistrés dans MLflow	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchRuns	Accorde l'autorisation de rechercher des essais qui répondent aux expressions	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchTraces	Accorde l'autorisation de rechercher des traces dans MLflow	Lecture	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetExperimentTag	Accorde l'autorisation de définir une étiquette sur une expérience	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetLoggedModelTags	Accorde l'autorisation de définir des balises pour un modèle connecté MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetModelVersionTag	Accorde l'autorisation de définir une balise pour la version du modèle	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetRegisteredModelAlias	Accorde l'autorisation de définir un alias de modèle enregistré	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetRegisteredModelTag	Accorde l'autorisation de définir une étiquette pour un modèle enregistré	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetTag	Accorde l'autorisation de définir un tag lors d'une course	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetTraceTag	Accorde l'autorisation de définir une balise de trace dans MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
StartTrace	Accorde l'autorisation de démarrer un traçage dans MLflow	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
TransitionModelVersionStage	Accorde l'autorisation de faire passer une version du modèle à une étape particulière	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateExperiment	Accorde l'autorisation de mettre à jour les métadonnées d'une MLflow expérience	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateModelVersion	Autorise la mise à jour de la version du modèle	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateRegisteredModel	Autorise la mise à jour d'un modèle enregistré	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateRun	Accorde l'autorisation de mettre à jour les métadonnées d'exécution	Écrire	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon SageMaker avec MLflow

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
mlflow-tracking-server	`arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-tracking-server/${MlflowTrackingServerName}`	

Clés de condition pour Amazon SageMaker avec MLflow

Amazon SageMaker with MLflow définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction d'une paire de clé et de valeur d'identification	String

Actions, ressources et clés de condition pour AWS Savings Plans

AWS Savings Plans (préfixe de service :`savingsplans`) fournit les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Savings Plans
- Types de ressources définis par AWS Savings Plans
- Clés de condition pour AWS Savings Plans

Actions définies par AWS Savings Plans

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSavingsPlan	Accorde l'autorisation de créer un Savings Plan (plan d'épargne)	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	Accorde l'autorisation de supprimer le Savings Plan (plan d'épargne) mis en file	Écriture	savingsplan*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	d'attente associé au compte client			aws:ResourceTag/${TagKey}	
DescribeSavingsPlanRates	Accorde l'autorisation de décrire les taux associés au Savings Plan (plan d'épargne) client	Lecture	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	Accorde l'autorisation de décrire les Savings Plans (plans d'épargne) associés au compte client	Lecture	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	Accorde l'autorisation de décrire les taux prévus par les Savings Plans (plans d'épargne)	Lecture			
DescribeSavingsPlansOfferings	Accorde l'autorisation de décrire les offres de Savings Plans (plans d'épargne) que le client est habilité à acheter	Lecture			
ListTagsForResource	Accorde l'autorisation d'afficher la liste des balises d'un Savings Plan (plan d'épargne)	List	savingsplan*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ReturnSavingsPlan	Autorise le remboursement d'un plan d'épargne	Écrire	savingsplan*		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation de baliser un Savings Plan (plan d'épargne)	Balisage	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'un Savings Plan (plan d'épargne)	Identification	savingsplan*		
				aws:TagKeys	

Types de ressources définis par AWS Savings Plans

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Savings Plans

AWS Savings Plans définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Secrets Manager

AWS Secrets Manager (préfixe de service :`secretsmanager`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Secrets Manager
- Types de ressources définis par AWS Secrets Manager
- Clés de condition pour AWS Secrets Manager

Actions définies par AWS Secrets Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetSecretValue	Octroie l'autorisation de récupérer et de déchiffrer une liste de secrets.	List			
CancelRotateSecret	Accorde l'autorisation d'annuler une rotation secrète en cours	Écrire	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotatio	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				nLambdaAr n secretsma nager:Res ourceTag/ tag-key aws:Resou rceTag/${ TagKey} secretsma nager:Sec retPrimar yRegion secretsma nager:res ource/ Type	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSecret	Accorde l'autorisation de créer un secret qui stocke les données chiffrées pouvant faire l'objet d'une interrogation et d'une rotation	Écrire	Secret*	secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:AddReplicaRegions secretsmanager:ForceOverwriteReplicaSecret secretsmanager:Type	
DeleteResourcePolicy	Accorde l'autorisation de supprimer la politique de ressource attachée à un secret	Gestion des autorisations	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
DeleteSecret	Accorde l'autorisation de supprimer un secret	Écrire	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
DescribeSecret	Accorde l'autorisation de récupérer les métadonnées relatives à un secret, mais pas les données chiffrées	Lecture	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRandomPassword	Accorde l'autorisation de générer une chaîne aléatoire pouvant être utilisée pour créer un mot de passe	Lecture			
GetResourcePolicy	Accorde l'autorisation d'obtenir la politique de ressource attachée à un secret	Lecture	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
GetSecretValue		Lecture	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de récupérer et de déchiffrer les données chiffrées				

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:resource/Type	
ListSecretVersionIds	Accorde l'autorisation de répertorier les versions disponibles d'un secret	Lecture	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSecrets	Accorde l'autorisation de répertorier les secrets disponibles	List			
PutResourcePolicy	Accorde l'autorisation d'attacher une politique de ressource à un secret	Gestion des autorisations	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion secretsmanager:res	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ource/ Type	
PutSecret Value	Accorde l'autorisation de créer une version du secret avec de nouvelles données chiffrées	Écrire	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RemoveRegionsFromReplication	Accorde l'autorisation de supprimer des régions de la réplication	Écrire	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ReplicateSecretToRegions	Accorde l'autorisation de convertir un secret existant en secret multi-région et de commencer à répliquer le secret dans une liste de nouvelles régions.	Écrire	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:ForceOverwriteReplicaSecret secretsmanager:resource/Type	
RestoreSecret	Accorde l'autorisation d'annuler la suppression d'un secret	Écrire	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
RotateSecret	Accorde l'autorisation de lancer la rotation d'un secret	Écrire	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:Mod	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ifyRotationRules secretsmanager:RotateImmediately secretsmanager:resource/Type secretsmanager:ExternalSecretRotationRoleArn	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StopReplicationToReplica	Accorde l'autorisation de supprimer le secret de la réplication et de promouvoir le secret en secret régional dans la région de réplique.	Écrire	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter des identifications à un secret	Identification	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:resource/Type	
UntagResource	Accorde l'autorisation de supprimer des identifications d'un secret	Identification	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSecret	Accorde l'autorisation de mettre à jour un secret avec de nouvelles métadonnées ou une nouvelle version des données chiffrées	Écrire	Secret*	secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretPrimaryRegion secretsmanager:Type secretsmanager:resource/Type	
UpdateSecretVersionStage	Accorde l'autorisation de déplacer une étape d'un secret vers un autre	Écrire	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:res	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ource/Type	
ValidateResourcePolicy	Accorde l'autorisation de valider une politique de ressource avant de l'attacher	Gestion des autorisations	Secret*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Types de ressources définis par AWS Secrets Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn secretsmanager:resource/Type

Clés de condition pour AWS Secrets Manager

AWS Secrets Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction d'une clé qui est présente dans la demande envoyée par l'utilisateur au service Secrets Manager	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la liste de tous les noms de clé d'identification présents dans la demande envoyée par l'utilisateur au service Secrets Manager	ArrayOfString
secretsmanager:AddReplicaRegions	Filtre l'accès en fonction de la liste des régions dans lesquelles répliquer le secret	ArrayOfString
secretsmanager:BlockPublicPolicy	Filtre l'accès selon que la politique de ressources bloque ou non Compte AWS l'accès étendu	Booléen
secretsmanager:Description	Filtre l'accès en fonction du texte de description présent dans la demande	String
secretsmanager:ExternalSecretRotationRoleArn	Filtre l'accès par le rôle de rotation secret externe géré (ARN) dans la demande	ARN
secretsmanager:ForceDeleteWithoutRecovery	Filtre l'accès selon que le secret doit être supprimé immédiatement ou non, sans aucune fenêtre de récupération	Booléen
secretsmanager:For	Filtre l'accès en fonction de l'écrasement d'un secret portant le même nom dans la région de destination	Booléen

Clés de condition	Description	Type
ceOverwriteReplicaSecret		
secretsmanager:KmsKeyArn	Filtre l'accès par la clé ARN de la clé KMS dans la demande	ARN
secretsmanager:KmsKeyId	Filtre l'accès en fonction de l'identifiant de clé de la clé KMS figurant dans la demande. Obsolète : utilisez secretsmanager : KmsKeyArn	String
secretsmanager:ModifyRotationRules	Filtre l'accès en fonction de la modification des règles de rotation du secret	Booléen
secretsmanager:Name	Filtre l'accès en fonction du nom convivial du secret présent dans la demande	String
secretsmanager:RecoveryWindowInDays	Filtre l'accès en fonction du nombre de jours pendant lesquels Secrets Manager attend avant de pouvoir supprimer le secret	Numérique
secretsmanager:ResourceTag/tag-key	Filtre l'accès en fonction d'une paire de clé et de valeur d'identification	String
secretsmanager:RotateImmediately	Filtre l'accès en fonction de la rotation immédiate du secret	Booléen
secretsmanager:RotationLambdaARN	Filtre l'accès en fonction de l'ARN de la fonction Lambda de rotation présent dans la demande	ARN

Clés de condition	Description	Type
secretsmanager:SecretId	Filtre l'accès en fonction de la valeur SecretID présente dans la demande	ARN
secretsmanager:SecretPrimaryRegion	Filtre l'accès par région principale dans laquelle le secret est créé s'il s'agit d'un secret multirégional	String
secretsmanager:Type	Filtre l'accès selon le type de secret externe géré dans la demande	String
secretsmanager:VersionId	Filtre l'accès en fonction de l'identifiant unique de la version du secret présent dans la demande	String
secretsmanager:VersionStage	Filtre l'accès en fonction de la liste des étapes de version présente dans la demande	String
secretsmanager:resource/AllowRotationLambdaArn	Filtre l'accès en fonction de l'ARN de la fonction Lambda de rotation associée au secret	ARN
secretsmanager:resource/Type	Filtre l'accès en fonction du type de secret externe géré associé au secret	String

Actions, ressources et clés de condition pour AWS Security Agent

AWS L'agent de sécurité (préfixe de service :`securityagent`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par l'agent AWS de sécurité
- Types de ressources définis par l'agent AWS de sécurité
- Clés de condition pour AWS Security Agent

Actions définies par l'agent AWS de sécurité

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddArtifact	Accorde l'autorisation d'ajouter un Artifact pour l'espace d'agent donné	Écrire	AgentSpace*		
BatchDeletePentests	Autorise la suppression de plusieurs tests de pénétration en une seule demande	Écrire	AgentSpace*		kms:Decrypt
BatchGetAgentSpaces	Accorde l'autorisation de récupérer plusieurs espaces d'agent en une seule demande	Lecture	AgentSpace*		kms:Decrypt
BatchGetArtifactMetadata	Accorde l'autorisation de récupérer un ou plusieurs enregistrements de	Lecture	AgentSpace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	métadonnées d'Artifact pour l'espace d'agent donné				
BatchGetFindings	Autorise la récupération de plusieurs résultats de tests de sécurité en une seule demande	Lecture	AgentSpace*		kms:Decrypt
BatchGetPentestJobContentMetadata	Accorde l'autorisation de récupérer les métadonnées du contenu de plusieurs tâches de pentest en une seule demande	Lecture	AgentSpace*		kms:Decrypt
BatchGetPentestJobTasks	Accorde l'autorisation de récupérer plusieurs tâches de pentest en une seule demande	Lecture	AgentSpace*		kms:Decrypt
BatchGetPentestJobs	Permet de récupérer plusieurs tâches de test de sécurité en une seule demande	Lecture	AgentSpace*		kms:Decrypt
BatchGetPentests	Autorise la récupération de plusieurs tests de pénétration en une seule demande	Lecture	AgentSpace*		kms:Decrypt
BatchGetTargetDomains	Accorde l'autorisation de récupérer plusieurs domaines cibles en une seule demande	Lecture	TargetDomain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAgentSpace	Accorde l'autorisation de créer un enregistrement d'espace agent	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	kms:Decrypt kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext
CreateApplication	Accorde l'autorisation de créer une application	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole kms:DescribeKey sso:CreateApplication
CreateDesignReview	Accorde l'autorisation de créer une révision de conception	Écrire	AgentSpace*		
CreateIntegration	Autorise la création d'une intégration de tests de sécurité	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMembership	Accorde l'autorisation d'ajouter un seul membre à un espace d'agent avec un rôle spécifié	Écrire	AgentSpace*		
CreateOneTimeLoginSession	Accorde l'autorisation de créer une session de connexion unique	Écrire	AgentSpace*		
CreatePentest	Autorise la création d'une nouvelle configuration de test d'intrusion	Écrire	AgentSpace*		kms:Decrypt
CreateSecurityRequirement	Accorde l'autorisation d'ajouter une exigence de sécurité gérée par le client	Écrire	SecurityRequirementPack*		
CreateTargetDomain	Accorde l'autorisation de créer un enregistrement de domaine cible	Écrire			
DeleteAgentSpace	Accorde l'autorisation de supprimer un enregistrement de l'espace agent	Écrire	AgentSpace*		kms:Decrypt
DeleteApplication	Autorise la suppression de l'application	Écrire	Application*		
DeleteArtifact	Accorde l'autorisation de supprimer un Artifact	Écrire	AgentSpace*		
DeleteDesignReview	Autorise la suppression d'une révision de conception	Écrire	AgentSpace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteIntegration	Accorde l'autorisation de supprimer l'intégration d'une application	Écrire	Integration*		
DeleteMembership	Accorde l'autorisation de supprimer un seul membre associé à un espace d'agent	Écrire	AgentSpace*		
DeleteSecurityRequirement	Accorde l'autorisation de supprimer une exigence de sécurité gérée par le client	Écrire	SecurityRequirementPack*		
DeleteTargetDomain	Accorde l'autorisation de supprimer un enregistrement de domaine cible	Écrire	TargetDomain*		
GetApplication	Accorde l'autorisation d'obtenir les détails de l'application par identifiant d'application	Lecture	Application*		
GetArtifact	Accorde l'autorisation de récupérer un Artifact pour l'espace d'agent donné	Lecture	AgentSpace*		
GetDesignReview	Accorde l'autorisation d'obtenir le statut de la révision de la conception de l'espace d'agent associée	Lecture	AgentSpace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDesignReviewArtifact	Accorde l'autorisation d'obtenir un artefact de révision de conception pour un document spécifique	Lecture	AgentSpace*		
GetDesignReviewFeedback	Accorde l'autorisation de recueillir des commentaires pour un commentaire de révision de conception	Lecture	AgentSpace*		
GetIntegration	Accorde l'autorisation d'obtenir les métadonnées d'intégration par identifiant	Lecture	Integration*		
GetSecurityRequirement	Accorde l'autorisation de récupérer une exigence de sécurité	Lecture	SecurityRequirementPack*		
InitiateProviderRegistration	Accorde l'autorisation d'initier l'enregistrement de l'application Security Agent pour le fournisseur donné (par exemple : GitHub)	Écrire			
ListAgentSpaces	Accorde l'autorisation de répertorier les espaces réservés aux agents	List			
ListApplications	Accorde l'autorisation de répertorier toutes les applications du compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListArtifacts	Accorde l'autorisation de répertorier tous les artefacts pour l'espace d'agent donné	List	AgentSpace*		
ListDesignReviewComments	Accorde l'autorisation de répertorier les commentaires relatifs aux révisions de conception	List	AgentSpace*		
ListDesignReviews	Permet de répertorier toutes les révisions de conception pour l'espace d'agent donné	List	AgentSpace*		
ListDiscoveredEndpoints	Accorde l'autorisation de répertorier les points de terminaison découverts associés à une tâche de pentest avec un filtrage optionnel par préfixe d'URI	List	AgentSpace*		kms:Decrypt
ListFindings	Permet de répertorier les résultats avec un support de filtrage et de pagination	List	AgentSpace*		kms:Decrypt
ListIntegratedResources	Accorde l'autorisation de répertorier les ressources intégrées pour un espace d'agent	List	AgentSpace*		
ListIntegrations	Accorde l'autorisation d'obtenir les intégrations détenues par l'appelant Compte AWS	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMemberships	Permet de répertorier tous les membres associés à un espace d'agent avec support de pagination	List	AgentSpace*		
ListPentestJobTasks	Permet de répertorier les tâches de pentest associées à une tâche de pentest	List	AgentSpace*		kms:Decrypt
ListPentestJobsForPentest	Permet de répertorier les offres d'emploi associées à un test d'intrusion	List	AgentSpace*		kms:Decrypt
ListPentests	Permet de répertorier les tests d'intrusion avec un filtrage optionnel par statut	List	AgentSpace*		kms:Decrypt
ListResourcesFromIntegration	Accorde l'autorisation de répertorier les ressources issues de l'intégration	List	Integration*		
ListSecurityRequirements	Accorde l'autorisation de répertorier toutes les exigences de sécurité	List	SecurityRequirementPack*		
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	AgentSpace		
			Application		
			Integration		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			SecurityRequirementPack		
			TargetDomain		
ListTargetDomains	Accorde l'autorisation de répertorier les domaines cibles	List			
PutDesignReviewFeedback	Accorde l'autorisation de soumettre des commentaires pour un commentaire de révision de conception	Écrire	AgentSpace*		
StartCodeRemediation	Autorise le lancement de la correction du code pour les résultats	Écrire	AgentSpace*		kms:Decrypt kms:GenerateDataKey
StartPentestJob	Autorise le lancement d'un test d'intrusion	Écrire	AgentSpace*		kms:Decrypt kms:GenerateDataKey
StopPentestJob	Autorise l'arrêt de l'exécution d'un test d'intrusion en cours	Écrire	AgentSpace*		kms:Decrypt

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Identification	AgentSpace		
			Application		
			Integration		
			SecurityRequirementPack		
			TargetDomain		
				aws:RequestTag/${TagKey} aws:TagKeys	
ToggleManagedSecurityRequirement	Accorde l'autorisation de changer le statut d'une exigence de sécurité gérée	Écrire	SecurityRequirementPack*		
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	AgentSpace		
			Application		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Integration		
			SecurityRequirementPack		
			TargetDomain		
				aws:TagKeys	
UpdateAgentSpace	Autorise la mise à jour d'un enregistrement d'espace agent	Écrire	AgentSpace*		kms:Decrypt
UpdateApplication	Accorde l'autorisation de mettre à jour la configuration de l'application	Écrire	Application*		iam:PassRole kms:DescribeKey
UpdateFinding	Autorise la mise à jour d'une constatation de sécurité existante avec de nouveaux détails ou un nouveau statut	Écrire	AgentSpace*		kms:Decrypt
UpdateIntegratedResources	Autorise la mise à jour des ressources intégrées pour un espace d'agent	Écrire	AgentSpace*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdatePentest	Autorise la mise à jour d'un test d'intrusion existant avec une nouvelle configuration ou de nouveaux paramètres	Écrire	AgentSpace*		kms:Decrypt
UpdateSecurityRequirement	Accorde l'autorisation de mettre à jour une exigence de sécurité gérée par le client	Écrire	SecurityRequirementPack*		
UpdateTargetDomain	Autorise la mise à jour d'un enregistrement de domaine cible	Écrire	TargetDomain*		
VerifyTargetDomain	Accorde l'autorisation de vérifier la propriété d'un domaine cible enregistré	Écrire	TargetDomain*		

Types de ressources définis par l'agent AWS de sécurité

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Application	arn:${Partition}:securityagent:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
SecurityRequirementPack	arn:${Partition}:securityagent:${Region}:${Account}:security-requirement-pack/${SecurityRequirementPackId}	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:securityagent:${Region}:${Account}:integration/${IntegrationId}	aws:ResourceTag/${TagKey}
AgentSpace	arn:${Partition}:securityagent:${Region}:${Account}:agent-space/${AgentId}	aws:ResourceTag/${TagKey}
TargetDomain	arn:${Partition}:securityagent:${Region}:${Account}:target-domain/${TargetDomainId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Security Agent

AWS L'agent de sécurité définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Security Hub

AWS Security Hub (préfixe de service :`securityhub`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Security Hub
- Types de ressources définis par AWS Security Hub
- Clés de condition pour AWS Security Hub

Actions définies par AWS Security Hub

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptAdministratorInvitation	Accorde l'autorisation d'accepter les invitations Security Hub à devenir un compte membre	Écriture	hub		
AcceptInvitation	Accorde l'autorisation d'accepter les invitations Security Hub à devenir un compte membre	Écrire	hub		
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de consigner la livraison des ressources	Gestion des autorisations	hub hubv2		
BatchDeleteAutomationRules	Accorde l'autorisation de supprimer une ou plusieurs règles d'automatisation dans Security Hub	Écrire	automation-rule*		
BatchDisableStandards	Accorde l'autorisation de désactiver les normes dans Security Hub	Écriture	hub		
BatchEnableStandards	Accorde l'autorisation d'activer les normes dans Security Hub	Écrire	hub		
BatchGetAutomationRules	Autorise Security Hub à récupérer une liste détaillée des règles d'automatisation en	Lecture	automation-rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	fonction de la règle Amazon Resource Names (ARNs)				
BatchGetConfigurationPolicyAssociations	Octroie l'autorisation de récupérer des informations sur les stratégies de configuration associées à une liste spécifique de comptes membres et d'unités organisationnelles de l'organisation du compte appelant.	Lecture			
BatchGetControlEvaluations [autorisation uniquement]	Accorde l'autorisation d'obtenir le statut d'activation et de conformité des contrôles, le nombre de résultats pour les contrôles et le score de sécurité global pour les contrôles sur la console Security Hub	Lecture	hub		
BatchGetSecurityControls	Octroie l'autorisation d'obtenir les informations relatives à des contrôles de sécurité spécifiques identifiés par un ID ou ARN	Lecture			securityhub:DescribeStandardsControls
BatchGetStandardsControlAssociations	Octroie l'autorisation d'obtenir le statut d'habilitation d'un lot de contrôles de sécurité dans les normes	Lecture			securityhub:DescribeStandardsControls

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchImportFindings	Accorde l'autorisation d'importer des résultats dans Security Hub à partir d'un produit intégré	Écrire	product*		
				securityhub:TargetAccount	
BatchUpdateAutomationRules	Accorde l'autorisation de mettre à jour une ou plusieurs règles d'automatisation depuis Security Hub en fonction de la règle Amazon Resource Names (ARNs) et des paramètres d'entrée	Écrire	automation-rule*		
BatchUpdateFindings	Accorde l'autorisation de mettre à jour des champs contrôlés par le client pour un ensemble sélectionné de résultats Security Hub	Écrire	hub		
			hubv2		
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath} securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdateStandardsControlAssociations	Octroie l'autorisation de mettre à jour le statut d'habilitation d'un lot de contrôles de sécurité dans les normes	Écrire			securityhub:UpdateStandardsControl
ConnectorRegistrationsV2	Accorde l'autorisation de terminer le flux de code d'autorisation OAuth 2.0 en fonction des paramètres d'entrée	Écrire			
CreateActionTarget	Accorde l'autorisation de créer des actions personnalisées dans Security Hub	Écrire	hub		
CreateAggregatorV2	Accorde l'autorisation de créer un AggregatorV2, qui configure l'agrégation des données entre les régions	Écrire			
CreateAutomationRule	Accorde l'autorisation de créer une règle d'automatisation basée sur les paramètres d'entrée	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAutomationRuleV2	Accorde l'autorisation de créer une règle d'automatisation V2 en fonction des paramètres d'entrée	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationPolicy	Octroie l'autorisation de créer une stratégie de configuration pour gérer les paramètres des membres de l'organisation dans Security Hub.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorV2	Accorde l'autorisation de créer un connecteur V2 en fonction des paramètres d'entrée	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	Accorde l'autorisation de à créer un agrégateur de recherche, qui contient la configuration d'agrégation de recherche entre régions	Écrire			
CreateInsight	Accorde l'autorisation de créer des informations dans Security Hub. Les aperçus sont des recueils de résultats connexes	Écriture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMembers	Accorde l'autorisation de créer des comptes de membres dans Security Hub	Écrire	hub		
CreateTicketV2	Accorde l'autorisation de créer un ticket pour une découverte OCSF sélectionnée	Écrire	connectorv2		
DeclineInvitations	Accorde l'autorisation de refuser les invitations Security Hub à devenir un compte membre	Écriture	hub		
DeleteActionTarget	Accorde l'autorisation de supprimer des actions personnalisées dans Security Hub	Écrire	hub		
DeleteAggregatorV2	Accorde l'autorisation de supprimer un AggregatorV2, qui configure l'agrégation des données entre les régions	Écrire	aggregatorv2*		
DeleteAutomationRuleV2	Autorise la suppression d'une règle d'automatisation V2 dans Security Hub	Écrire	automation-rulev2*		
DeleteConfigurationPolicy	Octroie l'autorisation de supprimer une stratégie de configuration existante.	Écrire	configuration-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConnectorV2	Autorise la suppression d'un connecteur V2 dans Security Hub	Écrire	connectorv2*		
DeleteFindingAggregator	Accorde l'autorisation de supprimer un agrégateur de recherche, ce qui désactive l'agrégation de recherche entre régions	Écrire	finding-aggregator*		
DeleteInsight	Accorde l'autorisation de supprimer des informations de Security Hub	Écriture	hub		
DeleteInvitations	Accorde l'autorisation de supprimer les invitations Security Hub à devenir un compte membre	Écriture	hub		
DeleteMembers	Accorde l'autorisation de supprimer des comptes membres de Security Hub	Écriture	hub		
DescribeActionTargets	Accorde l'autorisation de récupérer la liste des actions personnalisées à l'aide de l'API	Lecture	hub		
DescribeHub	Accorde l'autorisation de récupérer des informations sur la ressource de hub dans votre compte	Lecture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeOrganizationConfiguration	Accorde l'autorisation de décrire la configuration de l'organisation pour Security Hub	Lecture	hub		
DescribeProducts	Accorde l'autorisation de récupérer des informations sur les intégrations de produits Security Hub disponibles	Lecture	hub		
DescribeProductsV2	Autorise à récupérer des informations sur les intégrations de produits Security Hub V2 disponibles	Lecture	hubv2		
DescribeSecurityHubV2	Accorde l'autorisation de récupérer des informations sur la ressource Hub V2 de votre compte	Lecture			
DescribeStandards	Accorde l'autorisation de récupérer des informations sur les normes Security Hub	Lecture	hub		
DescribeStandardsControls	Accorde l'autorisation de récupérer des informations sur les contrôles des normes Security Hub	Lecture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableImportFindingsForProduct	Accorde l'autorisation de désactiver l'importation des résultats pour un produit intégré Security Hub	Écriture	hub		
DisableOrganizationAdminAccount	Accorde l'autorisation de supprimer le compte d'administrateur Security Hub de votre organisation	Écriture	hub		organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedAdministrators
DisableSecurityHub	Accorde l'autorisation de désactiver Security Hub	Écrire	hub		
DisableSecurityHubV2	Autorise la désactivation de Security Hub V2	Écrire			
DisassociateFromAdministratorAccount	Accorde à un compte membre Security Hub l'autorisation de se dissocier du compte administrateur associé	Écriture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateFromMasterAccount	Accorde l'autorisation à un compte membre Security Hub de se dissocier du compte principal associé	Écriture	hub		
DisassociateMembers	Accorde l'autorisation de dissocier des comptes membres Security Hub du compte administrateur associé	Écriture	hub		
EnableImportFindingsForProduct	Accorde l'autorisation d'activer l'importation des résultats pour un produit intégré Security Hub	Écriture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableOrganizationAdminAccount	Accorde l'autorisation de désigner un compte administrateur Security Hub pour votre organisation	Écriture	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Accorde l'autorisation d'activer Security Hub	Écrire	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableSecurityHubV2	Autorise l'activation de Security Hub V2	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
GetAdhocInsightResults [autorisation uniquement]	Autorise la récupération de données statistiques agrégées sur les résultats	Lecture	hub hubv2		
GetAdministratorAccount	Accorde l'autorisation de récupérer les informations relatives au compte administrateur Security Hub	Lecture	hub		
GetAggregatorV2	Accorde l'autorisation de récupérer les détails d'un AggregatorV2, qui configure l'agrégation des données entre les régions	Lecture	aggregatorv2*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAutomationRuleV2	Accorde l'autorisation de récupérer les détails d'une règle d'automatisation V2 depuis Security Hub sur la base de la règle Amazon Resource Name (ARN)	Lecture	automation-rulev2*		
GetConfigurationPolicy	Octroie l'autorisation d'obtenir un aperçu complet d'une stratégie de configuration créée par le compte appelant.	Lecture	configuration-policy*		
GetConfigurationPolicyAssociation	Octroie l'autorisation de récupérer des informations sur une stratégie de configuration associée à un compte membre ou une unité organisationnelle de l'organisation du compte appelant.	Lecture			
GetConnectorV2	Accorde l'autorisation de récupérer les détails d'un connecteur V2 à partir de Security Hub en fonction de l'identifiant du connecteur	Lecture	connectorv2*		
GetControlFindingSummary [autorisation uniquement]	Accorde l'autorisation de récupérer un score de sécurité et compte des statuts de recherche et de contrôle pour une norme de sécurité	Lecture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEnabledStandards	Accorde l'autorisation de récupérer la liste des normes activées dans Security Hub	List	hub		
GetFindingAggregator	Accorde l'autorisation de récupérer les détails d'un agrégateur de recherche, qui configure l'agrégation de recherche entre régions	Lecture	finding-aggregator*		
GetFindingHistory	Accorde l'autorisation de récupérer une liste de l'historique des résultats auprès de Security Hub	Lecture	hub		
GetFindings	Accorde l'autorisation de récupérer une liste de résultats à partir de Security Hub	Lecture	hub		
			hubv2		
GetFindingsTrendsV2	Donne l'autorisation de récupérer les tendances des résultats	Lecture	hubv2		
GetFreeTrialEndDate [autorisation uniquement]	Accorde l'autorisation de récupérer la date de fin de l'essai gratuit de Security Hub d'un compte	Lecture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFreeTrialUsage [autorisation uniquement]	Accorde l'autorisation de récupérer des informations sur l'utilisation de Security Hub pendant la période d'essai gratuite	Lecture	hub		
GetInsightFindingTrend [autorisation uniquement]	Accorde l'autorisation de récupérer une tendance de recherche d'informations à partir de Security Hub afin de générer un graphique	Lecture	hub		
GetInsightResults	Accorde l'autorisation de récupérer les résultats d'informations à partir de Security Hub	Lecture	hub		
GetInsights	Accorde l'autorisation de récupérer les informations de Security Hub	Liste	hub		
GetInvitationsCount	Accorde l'autorisation de récupérer le nombre d'invitations d'adhésion au Security Hub envoyées au compte	Lecture	hub		
GetMasterAccount	Accorde l'autorisation de récupérer des détails sur le compte principal Security Hub	Lecture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMembers	Accorde l'autorisation de récupérer les détails des comptes membres de Security Hub	Lecture	hub		
GetResourcesStatisticsV2	Accorde l'autorisation de récupérer des statistiques agrégées sur les ressources	Lecture	hubv2		
GetResourcesTrendsV2	Accorde l'autorisation de récupérer les tendances des ressources	Lecture	hubv2		
GetResourcesV2	Accorde l'autorisation de récupérer une liste de ressources	Lecture	hubv2		
GetSecurityControlDefinition	Octroie l'autorisation d'obtenir les informations de définition relatives à un contrôle de sécurité spécifique identifié par un ID.	Lecture			securityhub:DescribeStandardsControls
GetUsage [autorisation uniquement]	Accorde l'autorisation de récupérer des informations sur l'usage de Security Hub par les comptes	Lecture	hub		
InviteMembers	Autorise d'inviter d'autres AWS comptes à devenir des comptes membres du Security Hub	Écrire	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAggregatorsV2	Accorde l'autorisation de récupérer une liste d'AggregatorsV2, qui configure l'agrégation des données entre les régions	List			
ListAutomationRules	Accorde l'autorisation de récupérer une liste de règles d'automatisation et de leurs métadonnées pour le compte appelant à partir de Security Hub	List			
ListAutomationRulesV2	Accorde l'autorisation de récupérer une liste des règles d'automatisation V2 et leurs métadonnées pour le compte appelant depuis Security Hub	List			
ListConfigurationPolicies	Octroie l'autorisation de répertorier les récapitulatifs de toutes les stratégies de configuration créées par le compte appelant.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListConfigurationPolicyAssociations	Octroie l'autorisation de récupérer des informations sur toutes les stratégies de configuration associées à tous les comptes membres et unités organisationnelles de l'organisation du compte appelant.	List			
ListConnectorsV2	Accorde l'autorisation de récupérer une liste des connecteurs V2 et leurs métadonnées pour le compte appelant depuis Security Hub	List			
ListControlEvaluationSummaries [autorisation uniquement]	Accorde l'autorisation de récupérer une liste de contrôles pour une norme, y compris le contrôle IDs, les statuts et le nombre de résultats	Lecture	hub		
ListEnabledProductsForImport	Accorde l'autorisation de récupérer les produits intégrés Security Hub actuellement activés	List	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFindingAggregators	Accorde l'autorisation de récupérer une liste d'agrégateurs de recherche contenant la configuration d'agrégation de recherche entre régions	List			
ListInvitations	Accorde l'autorisation de récupérer les invitations Security Hub envoyées au compte	Liste	hub		
ListMembers	Accorde l'autorisation de récupérer les informations relatives aux comptes membres Security Hub associés au compte administrateur	Liste	hub		
ListOrganizationAdminAccounts	Accorde l'autorisation de répertorier les comptes administrateur Security Hub de votre organisation	List	hub		organizations:DescribeOrganization organizations:ListDelegatedAdministrators

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSecurityControlDefinitions	Octroie l'autorisation de récupérer une liste de définitions de contrôle de sécurité contenant des informations sur les contrôles de sécurité de la région actuelle	List			
ListStandardsControlAssociations	Octroie l'autorisation de répertorier le statut d'habilitation d'un contrôle de sécurité dans les normes	List			securityhub:DescribeStandardsControls
ListTagsForResource	Accorde l'autorisation de répertorier les balises associées à une ressource	Lecture	automation-rule		
			configuration-policy		
			hub		
SendFindingsEvents [autorisation uniquement]	Autorise l'utilisation d'une action personnalisée pour envoyer les résultats du Security Hub à Amazon EventBridge	Lecture	hub		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendInsightEvents [autorisation uniquement]	Autorise l'utilisation d'une action personnalisée pour envoyer des informations relatives au Security Hub à Amazon EventBridge	Lecture	hub		
StartConfigurationPolicyAssociation	Octroie l'autorisation d'associer une stratégie de configuration à un compte membre ou une unité organisationnelle dans l'organisation du compte appelant.	Écrire	hub		
StartConfigurationPolicyDisassociation	Octroie l'autorisation de supprimer une association de stratégie de configuration d'un compte membre ou d'une unité organisationnelle dans l'organisation du compte appelant.	Écrire	hub		
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource Security Hub	Balisage	aggregatorv2		
			automation-rule		
			automation-rulev2		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource Security Hub	Balisage	aggregatorv2		
			automation-rule		
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateActionTarget	Accorde l'autorisation de mettre à jour des actions personnalisées dans Security Hub	Écrire	hub		
UpdateAggregatorV2	Accorde l'autorisation de mettre à jour un AggregatorV2, qui configure l'agrégation des données entre les régions	Écrire	aggregatorv2*		
UpdateAutomationRuleV2	Autorise la mise à jour d'une règle d'automatisation V2 dans Security Hub en fonction de la règle Amazon Resource Name (ARN) et des paramètres d'entrée	Écrire	automation-rulev2*		
UpdateConfigurationPolicy	Octroie l'autorisation de mettre à jour une stratégie de configuration existante.	Écrire	configuration-policy*		
UpdateConnectorV2	Autorise la mise à jour d'un connecteur V2 dans Security Hub en fonction de l'identifiant du connecteur et des paramètres d'entrée	Écrire	connectorv2*		
UpdateFindingAggregator	Accorde l'autorisation de mettre à jour un agrégateur de recherche, qui contient la configuration d'agrégation de recherche entre régions	Écrire	finding-aggregator*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFindings	Accorde l'autorisation de mettre à jour les résultats de Security Hub	Écriture	hub		
UpdateInsight	Accorde l'autorisation de mettre à jour les informations dans Security Hub	Écriture	hub		
UpdateOrganizationConfiguration	Accorde l'autorisation de mettre à jour la configuration de l'organisation pour Security Hub	Écrire	hub		
UpdateSecurityControl	Octroie l'autorisation de mettre à jour les propriétés d'un contrôle de sécurité spécifique identifié par ID ou ARN.	Écrire			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	Accorde l'autorisation de mettre à jour la configuration de Security Hub	Écriture	hub		
UpdateStandardsControl	Accorde l'autorisation de mettre à jour les contrôles des normes Security Hub	Écrire	hub		

Types de ressources définis par AWS Security Hub

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
hub	arn:${Partition}:securityhub:${Region}:${Account}:hub/default	aws:ResourceTag/${TagKey}
hubv2	arn:${Partition}:securityhub:${Region}:${Account}:hubv2/${HubV2Id}	aws:ResourceTag/${TagKey}
product	arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}	
finding-aggregator	arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}	
aggregatorv2	arn:${Partition}:securityhub:${Region}:${Account}:aggregatorv2/${AggregatorV2Id}	aws:ResourceTag/${TagKey}
automation-rule	arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}	aws:ResourceTag/${TagKey}
automation-rulev2	arn:${Partition}:securityhub:${Region}:${Account}:automation-rulev2/${AutomationRuleV2Id}	aws:ResourceTag/${TagKey}
configuration-policy	arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}	aws:ResourceTag/${TagKey}
connectorv2	arn:${Partition}:securityhub:${Region}:${Account}:connectorv2/${ConnectorV2Id}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Security Hub

AWS Security Hub définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des actions basées sur la présence de paires clé-valeur de balise dans la requête	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des actions basées sur les paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des actions basées sur la présence de clés d'identification dans la requête	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	Filtre l'accès en fonction des champs et valeurs spécifiés dans la demande	String
securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	Filtre l'accès en fonction des champs et valeurs spécifiés dans la demande	String
securityhub:TargetAccount	Filtre l'accès en AwsAccountId fonction du champ spécifié dans la demande	String

Actions, ressources et clés de condition pour la réponse aux incidents AWS de sécurité

AWS Security Incident Response (préfixe de service :`security-ir`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Security Incident Response
- Types de ressources définis par AWS Security Incident Response
- Clés de condition pour AWS la réponse aux incidents de sécurité

Actions définies par AWS Security Incident Response

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetMemberAccountDetails	Accorde l'autorisation d'obtenir les détails du compte des membres par lots	Lecture	membership*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelMembership	Autorise l'annulation d'un abonnement	Écrire	membership*		
CloseCase	Autorise la clôture d'un dossier	Écrire	case*		
CreateCase	Accorde l'autorisation de créer un dossier	Écrire	case*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCaseComment	Accorde l'autorisation de créer un commentaire sur un dossier	Écrire	case*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMembership	Accorde l'autorisation de créer un abonnement	Écrire	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCase	Donne l'autorisation d'obtenir une affaire	Lecture	case*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCaseAttachmentDownloadUrl	Accorde l'autorisation d'obtenir l'URL de téléchargement d'une pièce jointe à un dossier	Lecture	case*		
GetCaseAttachmentUploadUrl	Accorde l'autorisation d'obtenir l'URL de téléchargement d'une pièce jointe au dossier	Écrire	case*		
GetMembership	Accorde l'autorisation de devenir membre	Lecture	membership*		
ListCaseEdits	Accorde l'autorisation de répertorier les modifications apportées aux dossiers	Lecture	case*		
ListCases	Accorde l'autorisation de répertorier les cas	List			
ListComments	Accorde l'autorisation de répertorier les commentaires relatifs au dossier	Lecture	case*		
ListInvestigations	Donne l'autorisation de répertorier les enquêtes relatives à une affaire	Lecture	case*		
ListMemberships	Accorde l'autorisation de répertorier les adhésions	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises qui sont attachées à la ressource spécifiée	Lecture	case membership		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
SendFeedback	Autorise l'envoi de commentaires sur les résultats de l'enquête	Écrire	case*		
TagResource	Accorde l'autorisation d'ajouter des balises à la ressource spécifiée	Identification	case		
			membership		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises de la ressource spécifiée	Identification	case		
			membership		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCase	Autorise la mise à jour d'un dossier	Écrire	case*		
UpdateCaseComment	Accorde l'autorisation de mettre à jour le commentaire d'un dossier	Écrire	case*		
UpdateCaseStatus	Accorde l'autorisation de mettre à jour le statut d'un dossier	Écrire	case*		
UpdateMembership	Accorde l'autorisation de mettre à jour les adhésions	Écrire	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganizationalUnit
UpdateResolverType	Autorise la mise à jour du type de résolveur de cas	Écrire	case*		

Types de ressources définis par AWS Security Incident Response

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
case	`arn:${Partition}:security-ir:${Region}:${Account}:case/${CaseId}`	aws:ResourceTag/${TagKey}
membership	`arn:${Partition}:security-ir:${Region}:${Account}:membership/${MembershipId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS la réponse aux incidents de sécurité

AWS Security Incident Response définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Security Lake

Amazon Security Lake (préfixe du service : `securitylake`) fournit les ressources, actions et clés de contexte de condition suivantes spécifiques au service en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Security Lake
- Types de ressources définis par Amazon Security Lake
- Clés de condition pour Amazon Security Lake

Actions définies par Amazon Security Lake

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAwsLogSource	Accorde l'autorisation d'activer n'importe quel type de source dans n'importe quelle région pour les comptes qui font partie d'une organisation de confiance ou les comptes autonomes.	Écrire	data-lake *		glue:CreateDatabase glue:CreateTable glue:GetDatabase glue:GetTable iam:CreateServiceLinkedRole kms:CreateGrant kms:DescribeKey
CreateCustomLogSource	Accorde l'autorisation d'ajouter une source personnalisée.	Écrire	data-lake *		glue:CreateCrawler glue:CreateDatabase glue:CreateTable

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					glue:StartCrawlerSchedule iam:DeleteRolePolicy iam:GetRole iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey kms:GenerateDataKey lakeformation:GrantPermissions lakeformation:Regi

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					sterResource s3:ListBucket s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataLake	Accorde l'autorisation de créer un nouveau lac de données de sécurité.	Écrire	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					lakeformation:GetDataLakeSettings lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListAccounts

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					organizations:ListDelegatedServicesForAccount s3:CreateBucket s3:GetObject s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					sqs:GetQueueAttributes sqs:SetQueueAttributes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeExceptionSubscription	Accorde l'autorisation de recevoir des notifications instantanées sur les exceptions. S'abonne aux rubriques SNS pour les notifications d'exceptions.	Écrire			
CreateDataLakeOrganizationConfiguration	Accorde l'autorisation d'activer automatiquement Amazon Security Lake pour les nouveaux comptes membres de votre organisation.	Écrire	data-lake*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSubscriber	Accorde l'autorisation de créer un abonné.	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:CreateRole iam:DeleteRolePolicy iam:GetRole iam:PutRolePolicy lakeformation:GrantPermissions lakeformation:ListPermissions lakeformation:RegisterResource lakeformation:RevokePermissions

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ram:GetResourceShareAssociations ram:GetResourceShares ram:UpdateResourceShare s3:PutObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSubscriberNotification	Accorde l'autorisation de créer une invocation de webhook pour informer un client de la présence de nouvelles données dans le lac de données.	Écrire	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:PassRole s3:GetBucketNotification s3:PutBucketNotification sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAwsLogSource	Accorde l'autorisation de désactiver n'importe quel type de source dans n'importe quelle région pour les comptes qui font partie d'une organisation de confiance ou les comptes autonomes.	Écrire	data-lake*		
DeleteCustomLogSource	Accorde l'autorisation de supprimer une source personnalisée.	Écrire	data-lake*		glue:StopCrawlerSchedule
DeleteDataLake	Accorde l'autorisation de supprimer un lac de données de sécurité.	Écrire	data-lake*		organizations:DescribeOrganization organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDataLakeExceptionSubscription	Accorde l'autorisation de se désabonner des rubriques SNS pour les notifications d'exception. Supprime les notifications d'exceptions de la rubrique SNS.	Écrire			
DeleteDataLakeOrganizationConfiguration	Accorde l'autorisation de supprimer l'activation automatique de l'accès à Amazon Security Lake pour les nouveaux comptes d'organisation.	Écrire	data-lake*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSubscriber	Accorde l'autorisation de supprimer l'abonné spécifié.	Écrire	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:GetRole iam:ListRolePolicies lakeformation:ListPermissions lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSubscriberNotification	Accorde l'autorisation de supprimer une invocation de webhook pour informer un client de la présence de nouvelles données dans le lac de données.	Écrire	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:GetRole iam:ListRolePolicies lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeregisterDataLakeDelegatedAdministrator	Accorde l'autorisation de supprimer le compte d'administrateur délégué et de désactiver Amazon Security Lake en tant que service pour cette organisation	Écrire			organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount
GetDataLakeExceptionSubscription	Accorde l'autorisation d'interroger le protocole et le point de terminaison qui ont été fournis lors de l'abonnement aux rubriques SNS pour les notifications d'exceptions.	Lecture			
GetDataLakeOrganizationConfiguration	Accorde l'autorisation d'obtenir les paramètres de configuration d'une organisation pour activer automatiquement l'accès à Amazon Security Lake pour les nouveaux comptes d'organisation	Lecture	data-lake*		organizations:DescribeOrganization

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataLakeSources	Accorde l'autorisation d'obtenir un instantané statique du lac de données de sécurité dans la région actuelle. L'instantané inclut les comptes activés et les sources de journaux.	Lecture	data-lake*		
GetSubscriber	Accorde l'autorisation d'obtenir des informations sur un abonné déjà créé.	Lecture	subscriber*		
ListDataLakeExceptions	Accorde l'autorisation d'obtenir la liste de tous les échecs ne pouvant pas être relancés.	List			
ListDataLakes	Accorde l'autorisation de répertorier les informations sur les lacs de données de sécurité.	List			
ListLogSources	Accorde l'autorisation d'afficher les comptes activés. Vous pouvez voir les sources activées dans les régions activées.	List			
ListSubscribers	Accorde l'autorisation de répertorier tous les abonnés.	List			
ListTagsForResource	Octroie l'autorisation de répertorier toutes les balises d'une ressource.	List	data-lake		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			subscriber		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterDataLakeDelegatedAdministrator	Accorde l'autorisation de désigner un compte comme compte administrateur Amazon Security Lake pour l'organisation.	Écrire			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount organizations:RegisterDelegatedAdministrator

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Octroie l'autorisation d'ajouter des balises à la ressource.	Identification	data-lake		
			subscriber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Octroie l'autorisation de supprimer des balises de la ressource.	Identification	data-lake		
			subscriber		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataLake	Accorde l'autorisation de mettre à jour un lac de données de sécurité.	Écrire	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetD

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ataLakeSettings lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					s3:CreateBucket s3:GetObject s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					sqs:SetQueueAttributes
UpdateDataLakeExceptionSubscription	Accorde l'autorisation de mettre à jour les abonnements aux rubriques SNS pour les notifications d'exception	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSubscriber	Accorde l'autorisation de mettre à jour un abonné.	Écrire	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:PutRolePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSubscriberNotification	Accorde l'autorisation de mettre à jour une invocation de webhook pour informer un client de la présence de nouvelles données dans le lac de données.	Écrire	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					iam:GetRole iam:PassRole iam:PutRolePolicy s3:CreateBucket s3:GetBucketNotification s3:ListBucket s3:PutBucketNotification s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					s3:PutLifecycleConfiguration sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Types de ressources définis par Amazon Security Lake

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
data-lake	`arn:${Partition}:securitylake:${Region}:${Account}:data-lake/default`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}
subscriber	`arn:${Partition}:securitylake:${Region}:${Account}:subscriber/${SubscriberId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Security Lake

Amazon Security Lake définit les clés de condition suivantes pouvant être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le service de migration de AWS serveurs

AWS Le service de migration de serveur (préfixe de service :`sms`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le service AWS de migration de serveurs
- Types de ressources définis par le service AWS de migration de serveurs
- Clés de condition pour le service AWS de migration de serveurs

Actions définies par le service AWS de migration de serveurs

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApp	Accorde l'autorisation de créer une configuration d'application pour migrer une application sur site vers AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReplicationJob	Accorde l'autorisation de créer une tâche pour migrer un serveur sur site vers AWS	Écrire			
DeleteApp	Accorde l'autorisation de supprimer une configuration d'application existante	Écriture			
DeleteAppLaunchConfiguration	Accorde l'autorisation de supprimer la configuration de lancement d'une application existante	Écriture			
DeleteAppReplicationConfiguration	Accorde l'autorisation de supprimer la configuration de réplication d'une application existante	Écriture			
DeleteAppValidationConfiguration	Accorde l'autorisation de supprimer la configuration de validation d'une application existante	Écrire			
DeleteReplicationJob	Accorde l'autorisation de supprimer une tâche existante vers laquelle migrer un serveur sur site AWS	Écrire			
DeleteServerCatalog	Autorise la suppression de la liste complète des serveurs sur site regroupés dans AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateConnector	Accorde l'autorisation de dissocier un connecteur qui a été associé	Écrire			
GenerateChangeSet	Accorde l'autorisation de générer un ChangeSet pour la CloudFormation pile d'une application	Écrire			
GenerateTemplate	Accorde l'autorisation de générer un CloudFormation modèle pour une application existante	Écrire			
GetApp	Accorde l'autorisation d'obtenir la configuration et les statuts d'une application existante	Lecture			
GetAppLaunchConfiguration	Accorde l'autorisation d'obtenir la configuration de lancement d'une application existante	Lecture			
GetAppReplicationConfiguration	Accorde l'autorisation d'obtenir la configuration de réplication d'une application existante	Lecture			
GetAppValidationConfiguration	Accorde l'autorisation d'obtenir la configuration de validation d'une application existante	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAppValidationOutput	Accorde l'autorisation d'obtenir une notification envoyée à partir d'un script de validation d'application	Lecture			
GetConnectors	Accorde l'autorisation d'obtenir tous les connecteurs qui ont été associés	Lecture			
GetMessages [autorisation uniquement]	Accorde l'autorisation de recevoir des messages du service de migration de AWS serveur vers le connecteur de migration de serveur	Lecture			
GetReplicationJobs	Accorde l'autorisation de transférer toutes les tâches existantes vers des serveurs sur site AWS	Lecture			
GetReplicationRuns	Accorde l'autorisation d'obtenir toutes les exécutions d'une tâche existante	Lecture			
GetServers	Accorde l'autorisation d'obtenir tous les serveurs qui ont été importés	Lecture			
ImportAppCatalog	Accorde l'autorisation d'importer le catalogue d' AWS applications depuis Application Discovery Service	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportServerCatalog	Accorde l'autorisation de rassembler une liste complète des serveurs sur site	Écrire			
LaunchApp	Accorde l'autorisation de créer et de lancer une CloudFormation pile pour une application existante	Écrire			
ListApps	Accorde l'autorisation d'obtenir une liste de résumés pour les applications existantes	Liste			
NotifyAppValidationOutput	Accorde l'autorisation d'envoyer une notification pour le script de validation d'application	Écriture			
PutAppLaunchConfiguration	Accorde l'autorisation de créer ou de mettre à jour la configuration de lancement d'une application existante.	Écriture			
PutAppReplicationConfiguration	Accorde l'autorisation de créer ou de mettre à jour la configuration de réplication d'une application existante.	Écriture			
PutAppValidationConfiguration	Accorde l'autorisation de mettre la configuration de validation d'une application existante	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendMessage [autorisation uniquement]	Accorde l'autorisation d'envoyer un message du connecteur de migration de AWS serveur au service de migration de serveur	Écrire			
StartAppReplication	Accorde l'autorisation de créer et de démarrer des tâches de réplication pour une application existante	Écriture			
StartOnDemandAppReplication	Accorde l'autorisation de démarrer une exécution de réplication pour une application existante	Écriture			
StartOnDemandReplicationRun	Accorde l'autorisation de démarrer une exécution de réplication pour une tâche de réplication existante	Écriture			
StopAppReplication	Accorde l'autorisation d'arrêter et de supprimer des tâches de réplication pour une application existante	Écrire			
TerminateApp	Accorde l'autorisation de mettre fin à la CloudFormation pile pour une application existante	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApp	Accorde l'autorisation de mettre à jour une configuration d'application existante	Écrire			
UpdateReplicationJob	Accorde l'autorisation de mettre à jour une tâche existante pour migrer un serveur sur site vers AWS	Écrire			

Types de ressources définis par le service AWS de migration de serveurs

AWS Le service de migration de serveur ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Server Migration Service, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le service AWS de migration de serveurs

ServerMigrationService ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Serverless Application Repository

AWS Serverless Application Repository (préfixe de service `serverlessrepo` :) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Serverless Application Repository
- Types de ressources définis par AWS Serverless Application Repository
- Clés de condition pour AWS Serverless Application Repository

Actions définies par AWS Serverless Application Repository

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateApplication	Accorde l'autorisation de créer une application, en incluant éventuellement un fichier AWS SAM pour créer la première version de l'application dans le même appel	Écrire			
CreateApplicationVersion	Accorde l'autorisation de créer une version d'application	Écrire	applications*		
CreateCloudFormationChangeSet	Accorde l'autorisation de créer un AWS CloudFormation ChangeSet pour l'application donnée	Écrire	applications*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				serverlessrepo:applicationType	
CreateCloudFormationTemplate	Accorde l'autorisation de créer un AWS CloudFormation modèle	Écrire	applications*		
				serverlessrepo:applicationType	
DeleteApplication	Accorde l'autorisation de supprimer l'application spécifiée	Écrire	applications*		
GetApplication	Accorde l'autorisation d'obtenir l'application spécifiée	Lecture	applications*		
				serverlessrepo:applicationType	
GetApplicationPolicy	Accorde l'autorisation d'obtenir la politique pour l'application spécifiée	Lecture	applications*		
GetCloudFormationTemplate	Accorde l'autorisation d'obtenir le AWS CloudFormation modèle spécifié	Lecture	applications*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplicationDependencies	Accorde l'autorisation de récupérer la liste des applications imbriquées dans l'application contenante	List	applications*		
				serverlessrepo:applicationType	
ListApplicationVersions	Accorde l'autorisation de répertorier les versions de l'application spécifiée appartenant au demandeur	List	applications*		
				serverlessrepo:applicationType	
ListApplications	Accorde l'autorisation de répertorier les applications appartenant au demandeur	List			
PutApplicationPolicy	Accorde l'autorisation de définir la politique pour l'application spécifiée	Écrire	applications*		
SearchApplications	Accorde l'autorisation d'obtenir toutes les applications autorisées pour cet utilisateur	Lecture		serverlessrepo:applicationType	
UnshareApplication	Accorde l'autorisation d'annuler le partage de l'application spécifiée	Écrire	applications*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApplication	Accorde l'autorisation de mettre à jour les métadonnées de l'application	Écrire	applications*		

Types de ressources définis par AWS Serverless Application Repository

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
applications	`arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}`	

Clés de condition pour AWS Serverless Application Repository

AWS Serverless Application Repository définit les clés de condition suivantes qui peuvent être utilisées dans `Condition` l'élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
serverlessrepo:applicationType	Filtre l'accès par type d'application	String

Actions, ressources et clés de condition pour le AWS service - Oracle Database@AWS

AWS Service - Oracle Database@AWS (préfixe de service :odb) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS service - Oracle Database@AWS
- Types de ressources définis par le AWS service - Oracle Database@AWS
- Clés de condition pour le AWS service - Oracle Database@AWS

Actions définies par le AWS service - Oracle Database@AWS

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptMarketplaceRegistration	Accorde l'autorisation d'enregistrer le jeton Amazon Web Services Marketplace pour votre compte Amazon Web Services afin d'activer votre abonnement Oracle Database @Amazon Web Services	Écrire			
CreateCloudAutonomousVmCluster	Accorde l'autorisation de créer un nouveau cluster de machines virtuelles autonomes dans l'infrastructure Exadata spécifiée	Écrire	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudExadataInfrastructure	Autorise la création d'une infrastructure Exadata	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCloudVmCluster	Accorde l'autorisation de créer un cluster de machines virtuelles sur l'infrastructure Exadata spécifiée	Écrire	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbNode [autorisation uniquement]	Accorde l'autorisation de créer un nœud de base de données	Écrire	db-node*		
CreateGrantShare [autorisation uniquement]	Accorde l'autorisation de créer un partage de subventions ODB	Écrire			
CreateOdbNetwork	Accorde l'autorisation de créer un réseau ODB	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateOdbPeeringConnection	Accorde l'autorisation de créer une connexion d'appairage ODB	Écrire	odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutboundIntegration [autorisation uniquement]	Accorde l'autorisation de créer une intégration sortante	Écrire	cloud-autonomous-vm-cluster*		
			cloud-vm-cluster*		
DeleteCloudAutonomousVmCluster	Accorde l'autorisation de supprimer un cluster de machines virtuelles autonomes	Écrire	cloud-autonomous-vm-cluster*		
DeleteCloudExadataInfrastructure	Accorde l'autorisation de supprimer une infrastructure Exadata spécifiée. Avant d'utiliser cette opération, assurez-vous de supprimer tous les clusters de machines virtuelles hébergés sur cette infrastructure Exadata	Écrire	cloud-exadata-infrastructure*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCloudVmCluster	Accorde l'autorisation de supprimer un cluster de machines virtuelles spécifié	Écrire	cloud-vm-cluster*		
DeleteDbNode [autorisation uniquement]	Accorde l'autorisation de supprimer un nœud de base de données	Écrire	db-node*		
DeleteGrantShare [autorisation uniquement]	Accorde l'autorisation de supprimer un partage de subvention ODB	Écrire			
DeleteOdbNetwork	Accorde l'autorisation de supprimer le réseau ODB spécifié	Écrire	odb-network*		
DeleteOdbPeeringConnection	Accorde l'autorisation de supprimer la connexion d'appairage ODB spécifiée. Lorsque vous supprimez une connexion d'appairage ODB, la connexion d'appairage VPC sous-jacente est également supprimée	Écrire	odb-peering-connection*		
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer une politique de ressource	Écrire	cloud-exadata-infrastructure*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			odb-network*		
GetCloudAutonomousVmCluster	Accorde l'autorisation d'obtenir des informations sur un cluster de machines virtuelles autonomes spécifique	Lecture	cloud-autonomous-vm-cluster*		
GetCloudExadataInfrastructure	Accorde l'autorisation d'obtenir des informations sur l'infrastructure Exadata spécifiée	Lecture	cloud-exadata-infrastructure*		
GetCloudExadataInfrastructureUnallocatedResources	Accorde l'autorisation de récupérer des informations sur les ressources non allouées dans une infrastructure Cloud Exadata spécifiée	Lecture	cloud-exadata-infrastructure*		
GetCloudVmCluster	Accorde l'autorisation d'obtenir des informations sur le cluster de machines virtuelles spécifié	Lecture	cloud-vm-cluster*		
GetDbNode	Accorde l'autorisation d'obtenir des informations sur le nœud de base de données spécifié	Lecture	cloud-vm-cluster*		
			db-node*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDbServer	Accorde l'autorisation d'obtenir des informations sur le serveur de base de données spécifié	Lecture	cloud-exadata-infrastructure*		
GetOciOnboardingStatus	Accorde l'autorisation d'obtenir le lien d'activation de la location et le statut d'intégration de votre compte Amazon Web Services	Lecture			
GetOdbNetwork	Accorde l'autorisation d'obtenir des informations sur le réseau ODB spécifié	Lecture	odb-network*		
GetOdbPeeringConnection	Accorde l'autorisation d'obtenir des informations sur la connexion ODB Peering spécifiée	Lecture	odb-peering-connection*		
GetResourcePolicy [autorisation uniquement]	Accorde l'autorisation d'obtenir une stratégie de ressource	Lecture	cloud-exadata-infrastructure*		
			odb-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InitializeService	Accorde l'autorisation d'initialiser le service ODB pour la première fois dans un compte	Écrire			
ListAutonomousVirtualMachines	Accorde l'autorisation de répertorier tous les appareils autonomes VMs dans un cluster de machines virtuelles autonomes	Lecture	cloud-autonomous-vm-cluster		
ListCloudAutonomousVmClusters	Accorde l'autorisation de répertorier tous les clusters de machines virtuelles autonomes dans une infrastructure Cloud Exadata spécifiée	List	cloud-exadata-infrastructure		
ListCloudExadataInfrastructures	Autorise à répertorier les informations relatives aux infrastructures Exadata détenues par votre compte Amazon Web Services	List			
ListCloudVmClusters	Autorise à répertorier les informations relatives aux clusters de machines virtuelles détenus par votre compte Amazon Web Services ou uniquement ceux de l'infrastructure Exadata spécifiée	List	cloud-exadata-infrastructure		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDbNodes	Accorde l'autorisation de répertorier les informations sur les nœuds de base de données pour le cluster de machines virtuelles spécifié	List	cloud-vm-cluster*		
ListDbServers	Accorde l'autorisation de répertorier les informations relatives aux serveurs de base de données appartenant à l'infrastructure Exadata spécifiée	Lecture	cloud-exadata-infrastructure*		
ListDbSystemShapes	Accorde l'autorisation de répertorier les informations relatives aux formes disponibles pour une infrastructure Exadata	Lecture			
ListGiVersions	Accorde l'autorisation de répertorier les informations relatives aux versions du logiciel Oracle Grid Infrastructure (GI) disponibles pour un cluster de machines virtuelles pour la forme spécifiée	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOdbNetworks	Autorise à répertorier les informations relatives aux réseaux ODB détenus par votre compte Amazon Web Services	List			
ListOdbPeeringConnections	Accorde l'autorisation de répertorier toutes les connexions de peering ODB ou celles associées à un réseau ODB spécifique	List	odb-network		
ListSystemVersions	Accorde l'autorisation de répertorier les informations sur les versions du système disponibles pour un cluster de machines virtuelles pour la GIVersion et la forme spécifiées	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les informations relatives aux balises appliquées à cette ressource	Lecture	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation de mettre à jour une politique de ressource.	Écrire	cloud-exadata-infrastructure*		
			odb-network*		
RebootDbNode	Accorde l'autorisation de redémarrer le nœud de base de données spécifié dans un cluster de machines virtuelles	Écrire	cloud-vm-cluster*		
			db-node*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDbNode	Accorde l'autorisation de démarrer le nœud de base de données spécifié dans un cluster de machines virtuelles	Écrire	cloud-vm-cluster*		
			db-node*		
StopDbNode	Accorde l'autorisation d'arrêter le nœud de base de données spécifié dans un cluster de machines virtuelles	Écrire	cloud-vm-cluster*		
TagResource	Accorde l'autorisation d'appliquer des balises à la ressource spécifiée	Identification	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			odb-peering-connection		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises de la ressource spécifiée	Identification	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCloudExadataInfrastructure	Autorise la mise à jour des propriétés d'une ressource d'infrastructure Exadata	Écrire	cloud-exadata-infrastructure*		
UpdateGrantShare [autorisation uniquement]	Accorde l'autorisation de mettre à jour une part de subvention ODB	Écrire			
UpdateOdbNetwork	Autorise la mise à jour des propriétés d'un réseau ODB spécifié	Écrire	odb-network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateOdbPeeringConnection	Autorise la mise à jour des propriétés d'une connexion d'appairage ODB spécifiée	Écrire	odb-peering-connection*		
UpdateOutboundIntegration [autorisation uniquement]	Autorise la mise à jour d'une intégration sortante	Écrire	cloud-autonomous-vm-cluster*		
			cloud-vm-cluster*		

Types de ressources définis par le AWS service - Oracle Database@AWS

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cloud-autonomous-vm-cluster	`arn:${Partition}:odb:${Region}:${Account}:cloud-autonomous-vm-cluster/${CloudAutonomousVmClusterId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
cloud-exadata-infrastructure	arn:${Partition}:odb:${Region}:${Account}:cloud-exadata-infrastructure/${CloudExadataInfrastructureId}	aws:ResourceTag/${TagKey}
cloud-vm-cluster	arn:${Partition}:odb:${Region}:${Account}:cloud-vm-cluster/${CloudVmClusterId}	aws:ResourceTag/${TagKey}
db-node	arn:${Partition}:odb:${Region}:${Account}:db-node/${DbNodeId}	aws:ResourceTag/${TagKey}
odb-network	arn:${Partition}:odb:${Region}:${Account}:odb-network/${OdbNetworkId}	aws:ResourceTag/${TagKey}
odb-peering-connection	arn:${Partition}:odb:${Region}:${Account}:odb-peering-connection/${OdbPeeringConnectionId}	aws:ResourceTag/${TagKey}

Clés de condition pour le AWS service - Oracle Database@AWS

AWS Service - Oracle Database@AWS définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS Service Catalog

AWS Service Catalog (préfixe de service :`servicecatalog`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Service Catalog
- Types de ressources définis par AWS Service Catalog
- Clés de condition pour AWS Service Catalog

Actions définies par AWS Service Catalog

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptPortfolioShare	Accorde l'autorisation d'accepter un portefeuille qui a été partagé avec vous	Écriture	Portfolio*		
AssociateAttributeGroup	Accorde l'autorisation d'associer un groupe d'attributs à une application	Écriture	Application* AttributeGroup*		
AssociateBudgetWithResource	Accorde l'autorisation d'associer un budget à une ressource	Écriture			
AssociatePrincipalWithPortfolio	Accorde l'autorisation d'associer un principal IAM à un portefeuille, ce qui donne au principal spécifié l'accès à tous les produits associés au portefeuille indiqué	Écriture	Portfolio*		
AssociateProductWithPortfolio	Accorde l'autorisation d'associer un produit à un portefeuille	Écriture			
AssociateResource	Accorde l'autorisation d'associer une ressource à une application	Écriture	Application*		cloudformation:DescribeStacks resource-groups:Cr

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					eateGroup resource-groups:GetGroup resource-groups:Tag
				servicecatalog:ResourceType servicecatalog:Resource	
AssociateServiceActionWithProvisioningArtifact	Accorde l'autorisation d'associer une action à un artefact de provisionnement	Écrire	Product*		
AssociateTagOptionWithResource	Accorde l'autorisation d'associer le produit spécifié TagOption au portefeuille ou au produit spécifié	Écrire	Portfolio		
			Product		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchAssociateServiceActionWithProvisioningArtifact	Accorde l'autorisation d'associer plusieurs actions en libre-service à des artefacts de provisionnement	Écriture			
BatchDisassociateServiceActionFromProvisioningArtifact	Accorde l'autorisation de dissocier un lot d'actions en libre-service de l'artefact de provisionnement spécifié	Écriture			
CopyProduct	Accorde l'autorisation de copier le produit source spécifié dans le produit cible indiqué ou dans un nouveau produit	Écriture			
CreateApplication	Accorde l'autorisation de créer une application	Écriture	Application*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAttributeGroup	Accorde l'autorisation de créer un groupe d'attributs	Écriture	AttributeGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConstraint	Accorde l'autorisation de créer une contrainte sur un produit et un portefeuille associés	Écriture	Product*		
CreatePortfolio	Accorde l'autorisation de créer un portefeuille	Écrire	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortfolioShare	Accorde l'autorisation de partager un portefeuille que vous possédez avec un autre Compte AWS	Gestion des autorisations	Portfolio*		
CreateProduct	Accorde l'autorisation de créer un produit et le premier artefact de provisionnement de ce produit	Écriture	Product*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedProductPlan	Accorde l'autorisation d'ajouter un nouveau plan de produit provisionné	Écriture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
CreateProvisioningArtifact	Accorde l'autorisation d'ajouter un nouvel artefact de provisionnement à un produit existant	Écriture	Product*		
CreateServiceAction	Accorde l'autorisation de créer une action en libre-service	Écrire			
CreateTagOption	Accorde l'autorisation de créer un TagOption	Écrire			
DeleteApplication	Accorde l'autorisation de supprimer une application si toutes les associations ont été supprimées de celle-ci	Écriture	Application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAttributeGroup	Accorde l'autorisation de supprimer un groupe d'attributs si toutes les associations ont été supprimées de celui-ci	Écriture	AttributeGroup*		
DeleteConstraint	Accorde l'autorisation de supprimer une contrainte existante d'un produit et d'un portefeuille associés	Écriture			
DeletePortfolio	Accorde l'autorisation de supprimer un portefeuille si toutes les associations et tous les partages ont été éliminés du portefeuille	Écrire	Portfolio*		
DeletePortfolioShare	Accorde l'autorisation d'annuler le partage d'un portefeuille que vous possédez et avec Compte AWS lequel vous l'avez déjà partagé	Gestion des autorisations	Portfolio*		
DeleteProduct	Accorde l'autorisation de supprimer un produit si toutes les associations ont été supprimées de celui-ci	Écriture	Product*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteProvisionedProductPlan	Accorde l'autorisation de supprimer un plan de produit provisionné	Écriture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DeleteProvisioningArtifact	Accorde l'autorisation de supprimer un artefact de provisionnement d'un produit	Écrire	Product*		
DeleteResourcePolicy [autorisation uniquement]	Accorde l'autorisation de supprimer une politique basée sur les ressources pour la ressource spécifiée	Écrire	Application		
			AttributeGroup		
DeleteServiceAction	Accorde l'autorisation de supprimer une action en libre-service	Écrire			
DeleteTagOption	Accorde l'autorisation de supprimer le fichier spécifié TagOption	Écrire			
DescribeConstraint	Accorde l'autorisation de décrire une contrainte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCopyProductStatus	Accorde l'autorisation d'obtenir le statut de l'opération de copie spécifiée	Lecture			
DescribePortfolio	Accorde l'autorisation de décrire un portefeuille	Lecture	Portfolio*		
DescribePortfolioShareStatus	Accorde l'autorisation d'obtenir le statut de l'opération de partage de portefeuille spécifiée	Lecture			
DescribePortfolioShares	Accorde l'autorisation d'afficher un résumé de chacun des partages de portefeuille créés pour le portefeuille spécifié	Liste	Portfolio*		
DescribeProduct	Accorde l'autorisation de décrire un produit en tant qu'utilisateur final	Lecture	Product*		
DescribeProductAsAdmin	Accorde l'autorisation de décrire un produit en tant qu'administrateur	Lecture	Product*		
DescribeProductView	Accorde l'autorisation de décrire un produit en tant qu'utilisateur final	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeProvisionedProduct	Accorde l'autorisation de décrire un produit provisionné	Lecture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisionedProductPlan	Accorde l'autorisation de décrire un plan de produit provisionné	Lecture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisioningArtifact	Accorde l'autorisation de décrire un artefact de provisionnement	Lecture	Product*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeProvisioningParameters	Accorde l'autorisation de décrire les paramètres à spécifier pour réussir la mise en service d'un artefact de provisionnement spécifié	Lecture	Product*		
DescribeRecord	Accorde l'autorisation de décrire un enregistrement et répertorie les sorties	Lecture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeServiceAction	Accorde l'autorisation de décrire une action en libre-service	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeServiceActionExecutionParameters	Accorde l'autorisation d'obtenir les paramètres par défaut si vous avez exécuté l'action de service spécifiée sur le produit provisionné spécifié	Lecture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeTagOption	Accorde l'autorisation d'obtenir des informations sur le paramètre spécifié TagOption	Lecture			
DisableAWSOrganizationsAccess	Accorde l'autorisation de désactiver le partage de portefeuille via la fonctionnalité AWS Organizations	Écrire			
DisassociateAttributeGroup	Accorde l'autorisation de dissocier un groupe d'attributs d'une application	Écriture	Application* AttributeGroup*		
DisassociateBudgetFromResource	Accorde l'autorisation de dissocier un budget d'une ressource	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociatePrincipalFromPortfolio	Accorde l'autorisation de dissocier un principal IAM d'un portefeuille	Écriture	Portfolio*		
DisassociateProductFromPortfolio	Accorde l'autorisation de dissocier un produit d'un portefeuille	Écriture			
DisassociateResource	Accorde l'autorisation de dissocier une ressource d'une application.	Écriture	Application*		resource-groups:DeleteGroup
				servicecatalog:ResourceType servicecatalog:Resource	
DisassociateServiceActionFromProvisioningArtifact	Accorde l'autorisation de dissocier l'association d'actions en libre-service spécifiée de l'artefact de provisionnement indiqué	Écrire	Product*		
DisassociateTagOptionFromResource	Accorde l'autorisation de dissocier la ressource spécifiée TagOption de la ressource spécifiée	Écrire	Portfolio		
			Product		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableAWSOrganizationsAccess	Accorde l'autorisation d'activer la fonctionnalité de partage de portefeuille via AWS Organizations	Écrire			
ExecuteProvisionedProductPlan	Accorde l'autorisation d'exécuter un plan de produit provisionné	Écriture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ExecuteProvisionedProductServiceAction	Accorde l'autorisation d'exécuter un plan de produit provisionné	Écrire		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAWSOrganizationsAccessStatus	Accorde l'autorisation d'obtenir le statut d'accès à la fonctionnalité de partage de portefeuille de AWS l'organisation	Lecture			
GetApplication	Accorde l'autorisation d'obtenir une application	Read	Application*		
GetAssociatedResource	Accorde l'autorisation d'obtenir des informations sur une ressource associée à une application	Read	Application*		
				servicecatalog:ResourceType servicecatalog:Resource	
GetAttributeGroup	Accorde l'autorisation d'obtenir un groupe d'attributs	Lecture	AttributeGroup*		
GetConfiguration	Accorde l'autorisation de lire AppRegistry les configurations	Lecture			
GetProvisionedProductOutputs	Accorde l'autorisation d'obtenir la sortie du produit provisionné avec l'ID ou le nom de celui-ci	Lecture			
GetResourcePolicy [autorisation uniquement]	Accorde l'autorisation d'obtenir une politique basée sur les ressources pour la ressource spécifiée	Lecture	Application		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Attribute Group		
ImportAsProvisionedProduct	Accorde l'autorisation d'importer une ressource dans un produit provisionné	Écriture	Product*		
ListAcceptedPortfolioShares	Accorde l'autorisation de répertorier les portefeuilles qui ont été partagés avec vous et que vous avez acceptés	List			
ListApplications	Accorde l'autorisation de répertorier vos applications	List			
ListAssociatedAttributeGroups	Accorde l'autorisation de répertorier les groupes d'attributs associés à une application	Liste	Application*		
ListAssociatedResources	Accorde l'autorisation de répertorier les ressources associées à une application	List	Application*		
ListAttributeGroups	Accorde l'autorisation de répertorier vos groupes d'attributs	List			
ListAttributeGroupsForApplication	Accorde l'autorisation de répertorier les groupes d'attributs associés pour une application donnée	List	Application*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBudgetsForResource	Accorde l'autorisation de répertorier tous les budgets associés à une ressource	Liste			
ListConstraintsForPortfolio	Accorde l'autorisation de répertorier les contraintes associées à un portefeuille donné	Liste			
ListLaunchPaths	Accorde l'autorisation de répertorier les différentes façons de lancer un produit donné en tant qu'utilisateur final	Liste	Product*		
ListOrganizationPortfolioAccess	Accorde l'autorisation de répertorier les nœuds d'organisation qui ont accès au portefeuille spécifié	List			
ListPortfolioAccess	Accorde l'autorisation de répertorier les AWS comptes avec lesquels vous avez partagé un portefeuille donné	List	Portfolio*		
ListPortfolios	Accorde l'autorisation de répertorier les portefeuilles de votre compte	Liste			
ListPortfoliosForProduct	Accorde l'autorisation de répertorier les portefeuilles associés à un produit donné	Liste	Product*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPrincipalsForPortfolio	Accorde l'autorisation de répertorier les mandataires IAM associés à un portefeuille donné	Liste	Portfolio*		
ListProvisionedProductPlans	Accorde l'autorisation de répertorier les plans de produits provisionnés	Liste		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListProvisioningArtifacts	Accorde l'autorisation de répertorier les artefacts de provisionnement associés à un produit donné	Liste	Product*		
ListProvisioningArtifactsForServiceAction	Accorde l'autorisation de répertorier tous les artefacts de provisionnement pour l'action en libre-service spécifiée	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRecordHistory	Accorde l'autorisation de répertorier tous les enregistrements de votre compte ou tous les enregistrements liés à un produit provisionné donné	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListResourcesForTagOption	Accorde l'autorisation de répertorier les ressources associées à la ressource spécifiée TagOption	List			
ListServiceActions	Accorde l'autorisation de répertorier toutes les actions en libre-service	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceActionsForProvisioningArtifact	Accorde l'autorisation de répertorier toutes les actions de service associées à l'artefact de provisionnement spécifié dans votre compte	Liste	Product*	servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListStackInstancesForProvisionedProduct	Accorde l'autorisation de répertorier le compte, la région et le statut de chaque instance de pile qui sont associés à un produit provisionné de type CFN_STACKSET	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListTagOptions	Accorde l'autorisation de répertorier les informations spécifiées TagOptions ou toutes TagOptions	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource appregistry de catalogue de services	Lecture	Application		
			Attribute Group		
NotifyProvisionProductEngineWorkflowResult	Accorde l'autorisation de notifier le résultat de l'exécution du moteur de provisionnement	Écrire			
NotifyTerminateProvisionedProductEngineWorkflowResult	Accorde l'autorisation de notifier le résultat de l'exécution du moteur de terminaison	Écrire			
NotifyUpdateProvisionedProductEngineWorkflowResult	Accorde l'autorisation de notifier le résultat de l'exécution du moteur de mise à jour	Écrire			
ProvisionProduct	Accorde l'autorisation de provisionner un produit avec un artefact de provisionnement spécifié et des paramètres de lancement	Écrire	Product*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutConfiguration	Accorde l'autorisation d'attribuer des AppRegistry configurations	Écrire			
PutResourcePolicy [autorisation uniquement]	Accorde l'autorisation d'ajouter une politique basée sur les ressources pour la ressource spécifiée	Écrire	Application		
			AttributeGroup		
RejectPortfolioShare	Accorde l'autorisation de rejeter un portefeuille qui a été partagé avec vous et que vous avez précédemment accepté	Écriture	Portfolio*		
ScanProvisionedProducts	Accorde l'autorisation de répertorier tous les produits provisionnés dans votre compte	Liste		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SearchProducts	Accorde l'autorisation de mettre en vente les produits mis à votre disposition en tant qu'utilisateur final	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SearchProductsAsAdmin	Accorde l'autorisation de répertorier tous les produits de votre compte ou tous les produits associés à un portefeuille donné	Liste			
SearchProvisionedProducts	Accorde l'autorisation de répertorier tous les produits provisionnés dans votre compte	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SyncResource	Accorde l'autorisation de synchroniser une ressource avec son état actuel dans AppRegistry	Écrire			cloudformation:UpdateStack
TagResource	Accorde l'autorisation de baliser une ressource appregistry de catalogue de service	Balisage	Application AttributeGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateProvisionedProduct	Accorde l'autorisation de résilier un produit provisionné existant	Écriture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource appregistry de catalogue de service	Balisage	Application		
			AttributeGroup		
				aws:TagKeys	
UpdateApplication	Accorde l'autorisation de mettre à jour les attributs d'une application existante	Écriture	Application*		iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAttributeGroup	Accorde l'autorisation de mettre à jour les attributs d'un groupe d'attributs existant	Écriture	AttributeGroup*		
UpdateConstraint	Accorde l'autorisation de mettre à jour les champs de métadonnées d'une contrainte existante	Écrire			
UpdatePortfolio	Autorise la mise à jour des and/or balises de champs de métadonnées d'un portefeuille existant	Écrire	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePortfolioShare	Accorde l'autorisation d'activer ou de désactiver le partage de ressources pour un partage de portefeuille existant	Gestion des autorisations	Portfolio*		
UpdateProduct	Autorise la mise à jour des and/or balises de champs de métadonnées d'un produit existant	Écrire	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateProvisionedProduct	Accorde l'autorisation de mettre à jour un produit provisionné existant	Écriture		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UpdateProvisionedProductProperties	Accorde l'autorisation de mettre à jour les propriétés d'un produit provisionné existant	Écriture			
UpdateProvisioningArtifact	Accorde l'autorisation de mettre à jour les champs de métadonnées d'un artefact de provisionnement existant	Écriture	Product*		
UpdateServiceAction	Accorde l'autorisation de mettre à jour une action en libre-service	Écrire			
UpdateTagOption	Accorde l'autorisation de mettre à jour le paramètre spécifié TagOption	Écrire			

Types de ressources définis par AWS Service Catalog

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Application	`arn:${Partition}:servicecatalog:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
Attribute Group	`arn:${Partition}:servicecatalog:${Region}:${Account}:/attribute-groups/${AttributeGroupId}`	aws:ResourceTag/${TagKey}
Portfolio	`arn:${Partition}:catalog:${Region}:${Account}:portfolio/${PortfolioId}`	aws:ResourceTag/${TagKey}
Product	`arn:${Partition}:catalog:${Region}:${Account}:product/${ProductId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Service Catalog

AWS Service Catalog définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

> **Note**
>
> Pour obtenir des exemples de politiques qui expliquent comment ces clés de condition peuvent être utilisées dans une politique IAM, consultez Exemples de politiques d'accès pour la gestion des produits provisionnés dans le Guide de l'administrateur .

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
servicecatalog:Resource	Filtre l'accès en contrôlant la valeur qui peut être spécifiée comme paramètre Resource dans une API de ressource AppRegistry associée	String
servicecatalog:ResourceType	Filtre l'accès en contrôlant la valeur qui peut être spécifiée comme ResourceType paramètre dans une API de ressource AppRegistry associée	String
servicecatalog:accountLevel	Filtre l'accès par utilisateur pour afficher et effectuer des actions sur les ressources créées par n'importe quel utilisateur du compte	String
servicecatalog:roleLevel	Filtre l'accès par utilisateur pour afficher et effectuer des actions sur les ressources créées par eux ou n'importe quel utilisateur endossant le même rôle qu'eux	String
servicecatalog:userLevel	Filtre l'accès par utilisateur pour afficher et effectuer des actions uniquement sur les ressources qu'ils ont créées	String

Actions, ressources et clés de condition pour les réseaux privés gérés fournissant des AWS services

AWS un service fournissant des réseaux privés gérés (préfixe de service :`private-networks`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS service fournissant des réseaux privés gérés
- Types de ressources définis par le AWS service fournissant des réseaux privés gérés
- Clés de condition pour les réseaux privés gérés fournissant des AWS services

Actions définies par le AWS service fournissant des réseaux privés gérés

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcknowledgeOrderReceipt	Accorde l'autorisation de reconnaître qu'un ordre a été reçu	Écrire	order*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateDeviceIdentifier	Accorde l'autorisation d'activer un identifiant de périphérique	Écrire	device-identifier*		
				aws:ResourceTag/${TagKey}	
ActivateNetworkSite	Accorde l'autorisation d'activer un site réseau	Écrire	network-site*		
			order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ConfigureAccessPoint	Accorde l'autorisation de configurer un point d'accès	Écrire	network-resource*		
CreateNetwork	Accorde l'autorisation de créer un réseau	Écrire	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkSite	Accorde l'autorisation de créer un site réseau	Écrire	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateDeviceIdentifier	Accorde l'autorisation de désactiver un identifiant de périphérique	Écrire	device-identifier*		
DeleteNetwork	Accorde l'autorisation de supprimer un réseau	Écrire	network*		
DeleteNetworkSite	Accorde l'autorisation de supprimer un site réseau	Écrire	network-site*		
GetDeviceIdentifier	Accorde l'autorisation d'obtenir un identifiant de périphérique	Lecture	device-identifier*		
				aws:ResourceTag/${TagKey}	
GetNetwork	Accorde l'autorisation d'obtenir un réseau	Lecture	network*		
				aws:ResourceTag/${TagKey}	
GetNetworkResource	Accorde l'autorisation d'obtenir une ressource réseau	Lecture	network-resource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetNetworkSite	Accorde l'autorisation d'obtenir un site réseau	Lecture	network-site*		
				aws:ResourceTag/${TagKey}	
GetOrder	Accorde l'autorisation d'obtenir une ordre de réseau	Lecture	order*		
				aws:ResourceTag/${TagKey}	
ListDeviceIdentifiers	Accorde l'autorisation de répertorier les identifiants de périphérique	List	network*		
ListNetworkResources	Accorde l'autorisation de répertorier les ressources réseau	List	network*		
ListNetworkSites	Accorde l'autorisation de répertorier les sites réseau	List	network*		
ListNetworks	Accorde l'autorisation de répertorier les réseaux	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOrders	Accorde l'autorisation de répertorier les ordres de réseau	List	network*		
ListTagsForResource	Accorde l'autorisation de renvoyer une liste d'étiquettes pour une ressource	List			
Ping	Accorde l'autorisation de vérifier l'état du service	Lecture			
StartNetworkResourceUpdate	Octroie l'autorisation de lancer une mise à jour sur la ressource réseau spécifiée	Écrire	network-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Accorde l'autorisation d'ajouter des balises à la ressource spécifiée	Identification	device-identifier		
			network		
			network-resource		
			network-site		
			order		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises de la ressource spécifiée	Identification	device-identifier		
			network		
			network-resource		
			network-site		
			order		
				aws:TagKeys	
UpdateNetworkSite	Accorde l'autorisation de mettre à jour un site réseau	Écrire	network-site*		
UpdateNetworkSitePlan	Accorde l'autorisation de mettre à jour un plan sur un site réseau	Écrire	network-site*		

Types de ressources définis par le AWS service fournissant des réseaux privés gérés

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
network	`arn:${Partition}:private-networks:${Region}:${Account}:network/${NetworkName}`	aws:ResourceTag/${TagKey}
network-site	`arn:${Partition}:private-networks:${Region}:${Account}:network-site/${NetworkName}/${NetworkSiteName}`	aws:ResourceTag/${TagKey}
network-resource	`arn:${Partition}:private-networks:${Region}:${Account}:network-resource/${NetworkName}/${ResourceId}`	aws:ResourceTag/${TagKey}
order	`arn:${Partition}:private-networks:${Region}:${Account}:order/${NetworkName}/${OrderId}`	aws:ResourceTag/${TagKey}
device-identifier	`arn:${Partition}:private-networks:${Region}:${Account}:device-identifier/${NetworkName}/${DeviceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les réseaux privés gérés fournissant des AWS services

AWS Un service fournissant des réseaux privés gérés définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en vérifiant la présence de paires clé-valeur de balise dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en vérifiant les paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Service Quotas

Service Quotas (préfixe de service : `servicequotas`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Service Quotas
- Types de ressources définis par Service Quotas
- Clés de condition pour Service Quotas

Actions définies par Service Quotas

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateServiceQuotaTemplate	Accorde l'autorisation d'associer le modèle Service Quotas à votre organisation	Écrire			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
CreateSupportCase	Accorde l'autorisation de soumettre une demande de création d'un dossier de support pour une demande d'augmentation de quota existante	Écrire			
DeleteServiceQuotaIncreaseRequestFromTemplate	Accorde l'autorisation de supprimer le quota de services spécifié du modèle de quota de services	Écriture			organizations:DescribeOrganization
DisassociateServiceQuotaTemplate	Accorde l'autorisation de dissocier le modèle Service Quotas de votre organisation	Écrire			organizations:DescribeOrganization

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAWSDefaultServiceQuota	Accorde l'autorisation de renvoyer les détails du quota de service spécifié, y compris la valeur AWS par défaut	Lecture			
GetAssociationForServiceQuotaTemplate	Accorde l'autorisation de récupérer la ServiceQuotaTemplateAssociationStatus valeur, qui vous indique si le modèle Service Quotas est associé à une organisation	Lecture			organizations:DescribeOrganization
GetAutoManagementConfiguration	Accorde l'autorisation de récupérer la gestion automatique de la configuration des Service Quotas, y compris les paramètres de notification, le type d'opt-in et les quotas exclus	Lecture			
GetQuotaUtilizationReport	Accorde l'autorisation de consulter le rapport généré	Lecture			
GetRequestedServiceQuotaChange	Accorde l'autorisation de récupérer les détails pour une demande d'augmentation de quota de services	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceQuota	Accorde l'autorisation de renvoyer les détails pour le quota de services spécifié, y compris la valeur appliquée	Lecture	quota		autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					route53:GetAccountLimit
				servicequotas:service	
GetServiceQuotaIncreaseRequestFromTemplate	Accorde l'autorisation de récupérer les détails pour une demande d'augmentation de quota de services à partir du modèle de quota de services	Lecture	quota		organizations:DescribeOrganization
				servicequotas:service	
ListAWSDefaultServiceQuotas	Accorde l'autorisation de répertorier tous les quotas de service par défaut pour le AWS service spécifié	Lecture			
ListRequestedServiceQuotaChangeHistory	Accorde l'autorisation de demander une liste des modifications apportées à des quotas pour un service	Lecture			
ListRequestedServiceQuotaChangeHistoryByQuota	Autorise la demande d'une liste des modifications apportés à des Service Quotas spécifiques	Lecture	quota		
				servicequotas:service	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceQuotaIncreaseRequestsInTemplate	Accorde l'autorisation de renvoyer une liste des demandes d'augmentation des quotas de services à partir du modèle de quota de services	Lecture			organizations:DescribeOrganization

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceQuotas	Accorde l'autorisation de répertorier tous les quotas de service pour le AWS service spécifié, dans ce compte, dans cette région	Lecture			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					route53:GetAccountLimit
ListServices	Accorde l'autorisation de répertorier les AWS services disponibles dans Service Quotas	Lecture			
ListTagsForResource	Accorde l'autorisation d'afficher les balises existantes sur une ressource SQ	Lecture			
PutServiceQuotaIncreaseRequestIntoTemplate	Accorde l'autorisation de définir et d'ajouter un quota au modèle de quota de services	Écriture	quota		organizations:DescribeOrganization
				servicequotas:service	
RequestServiceQuotaIncrease	Accorde l'autorisation d'envoyer la demande d'augmentation des quotas de services	Écrire	quota		
				servicequotas:service	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartAutoManagement	Accorde l'autorisation d'activer la gestion automatique des Quotas de Service pour une configuration Compte AWS, y compris les préférences de notification et les quotas exclus	Écrire			
StartQuotaUtilizationReport	Permet de demander l'utilisation des quotas et de créer un rapport pour votre compte	Lecture			
StopAutoManagement	Autorise l'arrêt de la gestion automatique des Quotas de Service pour un Compte AWS et la suppression de toutes les configurations associées	Écrire			
TagResource	Accorde l'autorisation d'associer un jeu de balises à une ressource SQ existante	Balisage		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer un jeu de balises d'une ressource SQ, lorsque les balises à supprimer correspondent à un ensemble de clés de balises fournies par le client	Identification		aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAutoManagement	Autorise la mise à jour de la gestion automatique de la configuration des Service Quotas, y compris les préférences de notification et les quotas exclus	Écrire			

Types de ressources définis par Service Quotas

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
quota	`arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}`	

Clés de condition pour Service Quotas

Service Quotas définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
servicequotas:service	Filtre l'accès par le AWS service spécifié	String

Actions, ressources et clés de condition pour Amazon SES

Amazon SES (préfixe de service : `ses`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon SES
- Types de ressources définis par Amazon SES
- Clés de condition pour Amazon SES

Actions définies par Amazon SES

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CloneReceiptRuleSet	Accorde l'autorisation de créer un ensemble de règles de réception en clonant une règle de réception existante.	Écriture		ses:ApiVersion	
CreateConfigurationSet	Accorde l'autorisation de créer un ensemble de configurations	Écriture		ses:ApiVersion	
CreateConfigurationSetEventDestination	Accorde l'autorisation de créer une destination d'événement d'ensemble de configurations	Écriture		ses:ApiVersion	
CreateConfigurationSetTrackingOptions	Accorde l'autorisation de créer une association entre un ensemble de configurations et un domaine personnalisé pour ouvrir et cliquer sur l'événement de suivi.	Écriture		ses:ApiVersion	
CreateCustomVerificationEmailTemplate	Accorde l'autorisation de créer un nouveau modèle d'e-mail de vérification personnalisé	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReceiptFilter	Accorde l'autorisation de créer un nouveau filtre d'adresse IP.	Écriture		ses:ApiVersion	
CreateReceiptRule	Accorde l'autorisation de créer une règle de réception.	Écriture		ses:ApiVersion	
CreateReceiptRuleSet	Accorde l'autorisation de créer un ensemble de règles de réception vide.	Écriture		ses:ApiVersion	
CreateTemplate	Accorde l'autorisation de créer un modèle d'e-mail.	Écriture		ses:ApiVersion	
DeleteConfigurationSet	Accorde l'autorisation de supprimer un ensemble de configurations existant	Écriture		ses:ApiVersion	
DeleteConfigurationSetEventDestination	Accorde l'autorisation de supprimer une destination d'événement	Écriture		ses:ApiVersion	
DeleteConfigurationSetTrackingOptions	Accorde l'autorisation de supprimer une association entre un ensemble de configurations et un domaine personnalisé pour ouvrir et cliquer sur l'événement de suivi.	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCustomVerificationEmailTemplate	Accorde l'autorisation de supprimer un modèle d'e-mail de vérification personnalisé existant	Écriture		ses:ApiVersion	
DeleteIdentity	Accorde l'autorisation de supprimer l'identité spécifiée.	Écriture		ses:ApiVersion	
DeleteIdentityPolicy	Accorde l'autorisation de supprimer la politique d'autorisation d'envoi spécifiée pour l'identité donnée (une adresse e-mail ou un domaine)	Gestion des autorisations		ses:ApiVersion	
DeleteReceiptFilter	Accorde l'autorisation de supprimer le filtre d'adresse IP spécifié.	Écriture		ses:ApiVersion	
DeleteReceiptRule	Accorde l'autorisation de supprimer la règle de réception spécifiée.	Écriture		ses:ApiVersion	
DeleteReceiptRuleSet	Accorde l'autorisation de supprimer l'ensemble de règles de réception spécifié et toutes les règles de réception qu'il contient.	Écriture		ses:ApiVersion	
DeleteTemplate	Accorde l'autorisation de supprimer un modèle d'e-mail	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteVerifiedEmailAddress	Accorde l'autorisation de supprimer l'adresse e-mail spécifiée à partir de la liste des adresses vérifiées.	Écriture		ses:ApiVersion	
DescribeActiveReceiptRuleSet	Accorde l'autorisation de renvoyer les métadonnées et les règles de réception de l'ensemble de règles de réception actuellement actif.	Lecture		ses:ApiVersion	
DescribeConfigurationSet	Accorde l'autorisation de renvoyer les détails de l'ensemble de configurations spécifié.	Lecture		ses:ApiVersion	
DescribeReceiptRule	Accorde l'autorisation de renvoyer les détails de la règle de réception spécifiée.	Lecture		ses:ApiVersion	
DescribeReceiptRuleSet	Accorde l'autorisation de renvoyer les détails de l'ensemble de règles de réception spécifié.	Lecture		ses:ApiVersion	
GetAccountSendingEnabled	Accorde l'autorisation de renvoyer l'état d'envoi d'e-mail de votre compte.	Lecture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCustomVerificationEmailTemplate	Accorde l'autorisation de renvoyer le modèle de vérification d'e-mail personnalisé pour le nom de modèle que vous spécifiez	Lecture		ses:ApiVersion	
GetIdentityDkimAttributes	Accorde l'autorisation de renvoyer l'état actuel de la signature Easy DKIM pour une entité.	Lecture		ses:ApiVersion	
GetIdentityMailFromDomainAttributes	Accorde l'autorisation de renvoyer les attributs MAIL FROM personnalisés pour une liste d'identités (adresses e-mail, and/or domaines)	Lecture		ses:ApiVersion	
GetIdentityNotificationAttributes	Accorde l'autorisation de renvoyer une structure décrivant les attributs de notification d'identité pour une liste d'identités vérifiées (and/or domaines d'adresses e-mail),	Lecture		ses:ApiVersion	
GetIdentityPolicies	Accorde l'autorisation de renvoyer les stratégies d'autorisation d'envoi demandées pour l'identité donnée (une adresse e-mail ou un domaine)	Lecture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetIdentityVerificationAttributes	Accorde l'autorisation de renvoyer l'état de vérification et (pour les identités de domaine) le jeton de vérification pour une liste d'identités.	Lecture		ses:ApiVersion	
GetSendQuota	Accorde l'autorisation de renvoyer les limites d'envoi actuelles de l'utilisateur.	Lecture		ses:ApiVersion	
GetSendStatistics	Accorde l'autorisation de renvoyer les statistiques d'envoi de l'utilisateur.	Lecture		ses:ApiVersion	
GetTemplate	Accorde l'autorisation de renvoyer le modèle d'objet (qui comprend la ligne d'Objet, la partie HTML et la partie de texte) du modèle que vous spécifiez.	Lecture		ses:ApiVersion	
ListConfigurationSets	Accorde l'autorisation de répertorier tous les ensembles de configurations pour votre compte	Liste		ses:ApiVersion	
ListCustomVerificationEmailTemplates	Accorde l'autorisation de répertorier tous les modèles d'e-mail de vérification personnalisés existant pour votre compte	Liste		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIdentities	Accorde l'autorisation de répertorier les identités d'e-mail de votre compte	Liste		ses:ApiVersion	
ListIdentityPolicies	Accorde l'autorisation de répertorier tous les modèles d'e-mail de votre compte	Liste		ses:ApiVersion	
ListReceiptFilters	Accorde l'autorisation de répertorier les filtres d'adresses IP associés à votre compte.	Lecture		ses:ApiVersion	
ListReceiptRuleSets	Accorde l'autorisation de répertorier les ensembles de règles de réception qui existent sous votre compte.	Lecture		ses:ApiVersion	
ListTemplates	Accorde l'autorisation de répertorier les modèles d'e-mail présents dans votre compte.	Liste		ses:ApiVersion	
ListVerifiedEmailAddresses	Accorde l'autorisation de répertorier toutes les adresses e-mail qui ont été vérifiées dans votre compte.	Lecture		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Accorde l'autorisation d'ajouter ou de mettre à jour les options de remise pour un ensemble de configurations.	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutIdentityPolicy	Accorde l'autorisation d'ajouter ou de mettre à jour une politique d'autorisation d'envoi pour l'identité spécifiée (une adresse e-mail ou un domaine).	Gestion des autorisations		ses:ApiVersion	
ReorderReceiptRuleSet	Accorde l'autorisation de réorganiser les règles de réception dans un ensemble de règles de réception.	Écriture		ses:ApiVersion	
SendBounce	Accorde l'autorisation de générer et d'envoyer un message de retour à l'expéditeur d'un e-mail que vous avez reçu via Amazon SES.	Écriture	identity*		
				ses:ApiVersion ses:FromAddress	
SendBulkTemplatedEmail	Accorde l'autorisation de composer un e-mail vers plusieurs destinations	Écriture	identity*		
			template*		
			configuration-set		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendCustomVerificationEmail	Accorde l'autorisation d'ajouter une adresse e-mail à la liste des identités et tente de la vérifier pour votre compte.	Écriture	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendEmail	Accorde l'autorisation d'envoyer un e-mail	Écriture	identity*		
			configuration-set		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendRawEmail	Accorde l'autorisation d'envoyer un e-mail avec l'en-tête et le contenu spécifiés par le client.	Écriture	identity*		
			configuration-set		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendTemplatedEmail	Accorde l'autorisation de rédiger un e-mail à l'aide d'un modèle d'e-mail.	Écriture	identity*		
			template*		
			configuration-set		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SetActiveReceiptRuleSet	Accorde l'autorisation de définir l'ensemble de règles de réception spécifié en tant que l'ensemble de règles de réception actif.	Écriture		ses:ApiVersion	
SetIdentityDkimEnabled	Accorde l'autorisation d'activer ou de désactiver la signature Easy DKIM d'un e-mail envoyé à partir d'une identité.	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetIdentityFeedbackForwardingEnabled	Accorde l'autorisation d'activer ou de désactiver le transfert par Amazon SES de notifications de retour et de réclamation pour une identité (une adresse e-mail ou un domaine).	Écriture		ses:ApiVersion	
SetIdentityHeadersInNotificationsEnabled	Accorde l'autorisation de définir si Amazon SES inclut les en-têtes de l'e-mail d'origine dans les notifications Amazon Simple Notification Service (Amazon SNS) d'un type spécifié pour une identité donnée (une adresse e-mail ou un domaine).	Écriture		ses:ApiVersion	
SetIdentityMailFromDomain	Accorde l'autorisation d'activer ou de désactiver la configuration personnalisée du domaine MAIL FROM pour une identité vérifiée.	Écriture		ses:ApiVersion	
SetIdentityNotificationTopic	Accorde l'autorisation de définir une rubrique Amazon Simple Notification Service (Amazon SNS) à utiliser lors de la remise des notifications pour une identité vérifiée.	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetReceiptRulePosition	Accorde l'autorisation de définir la position de la règle de réception spécifiée dans l'ensemble de règles de réception.	Écriture		ses:ApiVersion	
TestRenderTemplate	Accorde l'autorisation de créer un aperçu du contenu MIME d'un e-mail lorsqu'il est fourni avec un modèle et un jeu de données de remplacement	Écriture		ses:ApiVersion	
UpdateAccountSendingEnabled	Accorde l'autorisation d'activer ou de désactiver l'envoi d'e-mails pour votre compte.	Écriture		ses:ApiVersion	
UpdateConfigurationSetEventDestination	Accorde l'autorisation de mettre à jour la destination de l'événement d'un ensemble de configurations.	Écriture		ses:ApiVersion	
UpdateConfigurationSetReputationMetricsEnabled	Accorde l'autorisation d'activer ou de désactiver la publication de métriques de réputation pour les e-mails envoyés à l'aide d'un ensemble de configurations spécifique.	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConfigurationSetSendingEnabled	Accorde l'autorisation d'activer ou de désactiver l'envoi d'e-mails pour les messages envoyés à l'aide d'un ensemble de configurations spécifique.	Écriture		ses:ApiVersion	
UpdateConfigurationSetTrackingOptions	Accorde l'autorisation de modifier une association entre un ensemble de configurations et un domaine personnalisé pour ouvrir et cliquer sur l'événement de suivi.	Écriture		ses:ApiVersion	
UpdateCustomVerificationEmailTemplate	Accorde l'autorisation de mettre à jour un modèle d'e-mail de vérification personnalisé existant	Écriture		ses:ApiVersion	
UpdateReceiptRule	Accorde l'autorisation de mettre à jour une règle de réception.	Écriture		ses:ApiVersion	
UpdateTemplate	Accorde l'autorisation de mettre à jour un modèle d'e-mail	Écriture		ses:ApiVersion	
VerifyDomainDkim	Accorde l'autorisation de renvoyer un ensemble de jetons DKIM pour un domaine.	Écrire		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
VerifyDomainIdentity	Accorde l'autorisation de vérifier un domaine.	Écrire		ses:ApiVersion	
VerifyEmailAddress	Accorde l'autorisation de vérifier une adresse e-mail.	Écrire		ses:ApiVersion	
VerifyEmailIdentity	Accorde l'autorisation de vérifier une identité d'e-mail.	Écrire		ses:ApiVersion	

Types de ressources définis par Amazon SES

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}`	

Types de ressources	ARN	Clés de condition
identity	`arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}`	
template	`arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}`	

Clés de condition pour Amazon SES

Amazon SES définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
ses:ApiVersion	Filtre les actions en fonction de la version de l'API SES	String
ses:FeedbackAddress	Filtre les actions en fonction de l'adresse « Return-Path », qui spécifie l'adresse à laquelle les retours à l'expéditeur et les réclamations sont envoyés via le transfert de commentaires par e-mail	Chaîne
ses:FromAddress	Filtre les actions en fonction de l'adresse « From » d'un message	Chaîne
ses:FromDisplayName	Filtre les actions en fonction de l'adresse « From » utilisée comme nom d'affichage d'un message	Chaîne
ses:Recipients	Filtre les actions en fonction des adresses des destinataires d'un message, qui incluent les adresses « To », « CC » et « BCC »	ArrayOfString

Actions, ressources et clés de condition pour AWS Shield

AWS Shield (préfixe de service :`shield`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Shield
- Types de ressources définis par AWS Shield
- Clés de condition pour AWS Shield

Actions définies par AWS Shield

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateDRTLogBucket	Accorde l'autorisation d'autoriser l'équipe DDo S Response à accéder au compartiment Amazon S3 spécifié contenant vos journaux de flux	Écrire			s3:GetBucketPolicy s3:PutBucketPolicy

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateDRTRole	Accorde l'autorisation d'autoriser l'équipe DDo S Response, utilisant le rôle spécifié, à accéder à votre compte Compte AWS afin de vous aider à atténuer les attaques DDo S lors d'attaques potentielles	Écrire			iam:GetRole iam:ListAttachedRolePolicies iam:PassRole
AssociateHealthCheck	Accorde l'autorisation d'ajouter à la protection Shield Advanced une détection basée sur l'état pour une ressource.	Écrire	protection*		route53:GetHealthCheck
				aws:ResourceTag/${TagKey}	
AssociateProactiveEngagementDetails	Accorde l'autorisation d'initialiser un engagement proactif et de définir la liste de contacts que l'équipe DDo S Response (DRT) doit utiliser	Écrire			
CreateProtection	Accorde l'autorisation d'activer le service de protection DDo S pour un ARN de ressource donné	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateProtectionGroup	Accorde l'autorisation de créer un groupement de ressources protégées afin qu'elles puissent être traitées collectivement.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Accorde l'autorisation d'activer l'abonnement.	Écriture			
DeleteProtection	Accorde l'autorisation de supprimer une protection existante.	Écriture	protection*		
				aws:ResourceTag/${TagKey}	
DeleteProtectionGroup	Accorde l'autorisation de supprimer le groupe de protection spécifié.	Écriture	protection-group*		
				aws:ResourceTag/${TagKey}	
DeleteSubscription	Accorde l'autorisation de désactiver l'abonnement.	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAttack	Permet d'obtenir les détails de l'attaque. Pour protéger les détails des attaques par un groupe de règles géré DDo anti-S par AWS WAF, cette action appelle également wafv2 : DescribeTopContributorsByEvent pour récupérer les contributeurs aux attaques de la couche application, ce qui nécessite l'autorisation wafv2 : dans la politique IAM DescribeTopContributorsByEvent	Lecture	attack*		
DescribeAttackContributors [autorisation uniquement]	Permet d'obtenir des informations détaillées sur les contributeurs à une attaque DDo S spécifique	Lecture	attack*		
			protection-group		
DescribeAttackStatistics	Donne l'autorisation de décrire des informations sur le nombre et le type d'attaques détectées par AWS Shield au cours de l'année écoulée	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDRTAccess	Accorde l'autorisation de décrire le rôle actuel et la liste des buckets de log Amazon S3 utilisés par l'équipe DDo S Response pour accéder à vos fichiers Compte AWS tout en aidant à atténuer les attaques	Lecture			
DescribeEmergencyContactSettings	Accorde l'autorisation de lister les adresses e-mail que l'équipe DRT peut utiliser pour vous contacter lors d'une attaque suspectée.	Lecture			
DescribeProtection	Accorde l'autorisation d'obtenir des détails de protection.	Lecture	protection*		
				aws:ResourceTag/${TagKey}	
DescribeProtectionGroup	Accorde l'autorisation de décrire la spécification pour le groupe de protection spécifié.	Lecture	protection-group*		
				aws:ResourceTag/${TagKey}	
DescribeSubscription	Accorde l'autorisation d'obtenir les détails de l'abonnement, tels que l'heure de début.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableApplicationLayerAutomaticResponse	Accorde l'autorisation de désactiver la réponse automatique de la couche d'application pour la protection Shield Advanced d'une ressource	Écrire			
DisableProactiveEngagement	Accorde l'autorisation de retirer à l'équipe DDo S Response (DRT) l'autorisation d'informer les contacts des escalades	Écrire			
DisassociateDRTLogBucket	Accorde l'autorisation de supprimer l'accès de l'équipe DDo S Response au compartiment Amazon S3 spécifié contenant vos journaux de flux	Écrire			s3:DeleteBucketPolicy s3:GetBucketPolicy s3:PutBucketPolicy
DisassociateDRTRole	Accorde l'autorisation de supprimer l'accès de l'équipe DDo S Response à votre Compte AWS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateHealthCheck	Accorde l'autorisation de supprimer de la protection Shield Advanced une détection basée sur l'état pour une ressource.	Écrire	protection*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableApplicationLayerAutomaticResponse	Accorde l'autorisation d'activer la réponse automatique de la couche d'application pour la protection Shield Advanced d'une ressource	Écrire			apprunner:DescribeWebAclForService cloudfront:GetDistribution cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl iam:CreateServiceLinkedRole iam:GetRole wafv2:GetWebACL wafv2:GetWebACLForResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableProactiveEngagement	Accorde l'autorisation d'autoriser l'équipe DDo S Response (DRT) à utiliser le courrier électronique et le téléphone pour informer les contacts des escalades	Écrire			
GetGlobalThreatData [autorisation uniquement]	Autorise à récupérer les données et les tendances des renseignements sur les menaces mondiales à partir des systèmes de surveillance des menaces de AWS Shield	Lecture			
GetSubscriptionState	Accorde l'autorisation d'obtenir l'état de l'abonnement.	Lecture			
ListAttacks	Accorde l'autorisation de répertorier toutes les attaques existantes.	List			
ListMitigations [autorisation uniquement]	Accorde l'autorisation de récupérer une liste des mesures d'atténuation qui ont été appliquées lors d'attaques DDo S.	List	attack*		
ListProtectionGroups	Accorde l'autorisation de récupérer les groupes de protection pour le compte.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProtections	Accorde l'autorisation de répertorier toutes les protections existantes.	Liste			
ListResourcesInProtectionGroup	Accorde l'autorisation de récupérer les ressources incluses dans le groupe de protection.	List	protection-group*		
ListTagsForResource	Accorde l'autorisation d'obtenir des informations sur les AWS balises pour un Amazon Resource Name (ARN) spécifié dans AWS Shield	Lecture	protection		
			protection-group		
TagResource	Autorise l'ajout ou la mise à jour de balises pour une ressource dans AWS Shield	Identification	protection		
			protection-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises d'une ressource dans AWS Shield	Identification	protection		
			protection-group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateApplicationLayerAutomaticResponse	Accorde l'autorisation de mettre à jour la réponse automatique de la couche d'application pour la protection Shield Advanced d'une ressource	Écrire			apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL wafv2:GetWebACLForResource
UpdateEmergencyContactSettings	Accorde l'autorisation de mettre à jour les détails de la liste des adresses e-mail que l'équipe DRT peut utiliser pour vous contacter lors d'une attaque suspectée.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateProtectionGroup	Accorde l'autorisation de mettre à jour un groupe de protection existant.	Écriture	protection-group*		
				aws:ResourceTag/${TagKey}	
UpdateSubscription	Accorde l'autorisation de mettre à jour les détails d'un abonnement existant.	Écrire			

Types de ressources définis par AWS Shield

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
attack	`arn:${Partition}:shield::${Account}:attack/${Id}`	
protection	`arn:${Partition}:shield::${Account}:protection/${Id}`	aws:ResourceTag/${TagKey}
protection-group	`arn:${Partition}:shield::${Account}:protection-group/${Id}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Shield

AWS Shield définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour le directeur de la sécurité du réseau AWS Shield

AWS Le directeur de sécurité réseau Shield (préfixe de service :`network-security-director`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le directeur de la sécurité du réseau AWS Shield
- Types de ressources définis par le directeur de la sécurité du réseau AWS Shield
- Clés de condition pour le directeur de la sécurité du réseau AWS Shield

Actions définies par le directeur de la sécurité du réseau AWS Shield

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetFinding	Donne l'autorisation d'obtenir un résultat	Lecture			
GetResource	Accorde l'autorisation d'obtenir une ressource	Lecture			
ListAccountSummaries	Accorde l'autorisation de répertorier les résumés des comptes pour un compte	List			
ListFindings	Donne l'autorisation de répertorier les résultats	List			
ListInsights	Autorise à répertorier les informations relatives à la dernière analyse de sécurité du réseau	List			
ListRemediations	Accorde l'autorisation de répertorier les corrections apportées à une constatation	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResources	Accorde l'autorisation de répertorier les ressources	List			
UpdateFinding	Accorde l'autorisation de mettre à jour le statut d'une découverte	Écrire			

Types de ressources définis par le directeur de la sécurité du réseau AWS Shield

AWS Le directeur de la sécurité réseau de Shield ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès au directeur de sécurité du réseau AWS Shield, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour le directeur de la sécurité du réseau AWS Shield

Network Security Director ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le AWS signataire

AWS Le signataire (préfixe de service :`signer`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS signataire
- Types de ressources définis par le AWS signataire
- Clés de condition pour le AWS signataire

Actions définies par le AWS signataire

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddProfilePermission	Accorde l'autorisation d'ajouter des autorisations entre comptes à un profil de signature	Gestion des autorisations	signing-profile*		
CancelSigningProfile	Accorde l'autorisation de remplacer l'état d'un profil de signature par ANNULÉ	Écriture	signing-profile*		
				signer:ProfileVersion	
DescribeSigningJob	Accorde l'autorisation de renvoyer les informations sur une tâche de signature spécifique	Lecture	signing-job*		
GetRevocationStatus	Accorde l'autorisation d'interroger les informations relatives à la révocation des ressources de signature	Lecture	signing-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			signing-profile*		
GetSigningPlatform	Accorde l'autorisation de renvoyer les informations sur une plateforme de signature spécifique	Lecture			
GetSigningProfile	Accorde l'autorisation de renvoyer les informations sur un profil de signature spécifique	Lecture	signing-profile*		
				signer:ProfileVersion	
ListProfilePermissions	Accorde l'autorisation de répertorier les autorisations entre comptes associées à un profil de signature	Lecture	signing-profile*		
ListSigningJobs	Accorde l'autorisation de répertorier toutes les tâches de signature dans votre compte	Liste			
ListSigningPlatforms	Accorde l'autorisation de répertorier toutes les plateformes de signature disponibles	Liste			
ListSigningProfiles	Accorde l'autorisation de répertorier tous les profils de signature dans votre compte	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises associées à un profil de signature	Lecture	signing-profile*		
PutSigningProfile	Accorde l'autorisation de créer un profil de signature	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveProfilePermission	Accorde l'autorisation de supprimer les autorisations entre comptes d'un profil de signature	Gestion des autorisations	signing-profile*		
RevokeSignature	Accorde l'autorisation de remplacer l'état d'une tâche de signature par REVOQUÉ	Écriture	signing-job*		
				signer:ProfileVersion	
RevokeSigningProfile	Accorde l'autorisation de remplacer l'état d'un profil de signature par REVOQUÉ	Écrire	signing-profile*		
				signer:ProfileVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SignPayload	Accorde l'autorisation de lancer une tâche de signature sur la charge utile fournie	Écrire	signing-profile*		
				signer:ProfileVersion	
StartSigningJob	Accorde l'autorisation de lancer une tâche de signature sur le code fourni	Écriture	signing-profile*		
				signer:ProfileVersion	
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à un profil de signature	Balisage	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'un profil de signature	Identification	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Types de ressources définis par le AWS signataire

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
signing-profile	`arn:${Partition}:signer:${Region}:${Account}:/signing-profiles/${ProfileName}`	aws:ResourceTag/${TagKey}
signing-job	`arn:${Partition}:signer:${Region}:${Account}:/signing-jobs/${JobId}`	

Clés de condition pour le AWS signataire

AWS Le signataire définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des étiquettes	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction de la présence d'étiquettes obligatoires dans la demande	ArrayOfString
signer:ProfileVersion	Filtre l'accès en fonction de la version du profil de signature	String

Actions, ressources et clés de condition pour la AWS connexion

AWS Signin (préfixe de service :`signin`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Signin
- Types de ressources définis par AWS Signin
- Clés de condition pour la AWS connexion

Actions définies par AWS Signin

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AuthorizeOAuth2Access	Accorde l'autorisation de s'authentifier via un navigateur et d'obtenir un code d'autorisation OAuth 2.0 pour l'échange d'informations d'identification	Lecture	oauth2-public-client-localhost*		
			oauth2-public-client-remote*		
CreateOAuth2Token	Autorise l'échange d'un code d'autorisation contre un jeton d'accès OAuth 2.0 et un jeton d'actualisation qui peuvent être utilisés pour accéder aux AWS services à partir d'outils et d'applications de développement	Lecture	oauth2-public-client-localhost*		
			oauth2-public-client-remote*		
CreateTrustedIdentityPropagationApplicationForConsole	Accorde l'autorisation de créer une application Identity Center qui représente AWS Management Console l'instance d'une organisation Identity Center	Écrire			sso:CreateApplication sso:GetSharedSsoConfiguration

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					sso:ListApplications sso:PutApplicationAccessScope sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTrustedIdentityPropagationApplicationsForConsole	Accorde l'autorisation de répertorier toutes les applications Identity Center qui représentent AWS Management Console	List			sso:GetSharedSsoConfiguration sso:ListApplications

Types de ressources définis par AWS Signin

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
oauth2-public-client-localhost	`arn:${Partition}:signin:${Region}:${Account}:oauth2/public-client/localhost`	
oauth2-public-client-remote	`arn:${Partition}:signin:${Region}:${Account}:oauth2/public-client/remote`	

Clés de condition pour la AWS connexion

Signin ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Simple Email Service - Mail Manager

Amazon Simple Email Service - Mail Manager (préfixe de service :`ses`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Simple Email Service - Mail Manager
- Types de ressources définis par Amazon Simple Email Service - Mail Manager
- Clés de condition pour Amazon Simple Email Service - Mail Manager

Actions définies par Amazon Simple Email Service - Mail Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux vendus pour les ressources de Mail Manager	Gestion des autorisations	mailmanager-ingress-point		
			mailmanager-rule-set		
CreateAddonInstance	Accorde l'autorisation de créer une instance d'addon	Écrire		aws:RequestTag/${TagKey} aws:TagKeys ses:AddonSubscriptionArn	
CreateAddonSubscription	Accorde l'autorisation de créer un abonnement complémentaire	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAddressList	Accorde l'autorisation de créer une liste d'adresses	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAddressListImportJob	Accorde l'autorisation de créer une tâche d'importation dans une liste d'adresses	Écrire	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
CreateArchive	Accorde l'autorisation de créer une archive	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngressPoint	Accorde l'autorisation de créer un point d'entrée	Écrire		aws:RequestTag/${TagKey} aws:TagKeys ses:MailManagerRuleSetArn ses:MailManagerTrafficPolicyArn	ec2:DescribeVpcEndpoints iam:CreateServiceLinkedRole
CreateRelay	Accorde l'autorisation de créer un relais SMTP	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRuleSet	Accorde l'autorisation de créer un ensemble de règles	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrafficPolicy	Accorde l'autorisation de créer une politique de trafic	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddonInstance	Accorde l'autorisation de supprimer une instance d'addon	Écrire	addon-instance*		
				aws:RequestTag/${TagKey}	
DeleteAddonSubscription	Accorde l'autorisation de supprimer un abonnement à un module complémentaire	Écrire	addon-subscription*		
				aws:RequestTag/${TagKey}	
DeleteAddressList	Accorde l'autorisation de supprimer une liste d'adresses	Écrire	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteArchive	Accorde l'autorisation de supprimer une archive.	Écrire	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
DeleteIngressPoint	Autorise la suppression d'un point d'entrée	Écrire	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
DeleteRelay	Accorde l'autorisation de supprimer un relais SMTP	Écrire	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
DeleteRuleSet	Accorde l'autorisation de supprimer un ensemble de règles	Écrire	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTrafficPolicy	Autorise la suppression d'un point de trafic	Écrire	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	
DeregisterMemberFromAddressList	Accorde l'autorisation de supprimer un membre d'une liste d'adresses	Écrire	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetAddonInstance	Accorde l'autorisation d'obtenir des informations sur une instance d'addon	Lecture	addon-instance*		
				aws:RequestTag/${TagKey}	
GetAddonSubscription	Accorde l'autorisation d'obtenir des informations sur un abonnement à un module complémentaire	Lecture	addon-subscription*		
				aws:RequestTag/${TagKey}	
GetAddressList	Accorde l'autorisation d'obtenir des informations sur une liste d'adresses	Lecture	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAddressListImportJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'importation dans une liste d'adresses	Lecture	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetArchive	Accorde l'autorisation d'obtenir des informations sur une archive	Lecture	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
GetArchiveExport	Accorde l'autorisation d'obtenir des informations sur l'exportation d'une archive	Lecture	mailmanager-archive*		
GetArchiveMessage	Accorde l'autorisation de récupérer le message archivé	Lecture	mailmanager-archive*		
GetArchiveMessageContent	Accorde l'autorisation de récupérer le contenu des messages archivés	Lecture	mailmanager-archive*		
GetArchiveSearch	Accorde l'autorisation d'obtenir des informations sur une recherche	Lecture	mailmanager-archive*		
GetArchiveSearchResults	Accorde l'autorisation d'obtenir des informations sur les résultats de recherche	Lecture	mailmanager-archive*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetIngressPoint	Accorde l'autorisation d'obtenir des informations sur un point d'entrée	Lecture	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	
GetMemberOfAddressList	Accorde l'autorisation d'obtenir des informations sur un membre dans une liste d'adresses	Lecture	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetRelay	Accorde l'autorisation d'obtenir des informations sur un relais SMTP	Lecture	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
GetRuleSet	Accorde l'autorisation d'obtenir des informations sur un ensemble de règles	Lecture	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
GetTrafficPolicy	Accorde l'autorisation d'obtenir des informations sur une politique de trafic	Lecture	mailmanager-traffic-policy*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey}	
ListAddonInstances	Accorde l'autorisation de répertorier toutes les instances d'addon associées à votre compte	List			
ListAddonSubscriptions	Permet de répertorier tous les abonnements complémentaires associés à votre compte	List			
ListAddressListImportJobs	Accorde l'autorisation de répertorier toutes les tâches d'importation associées à une liste d'adresses	List	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListAddressLists	Permet de répertorier toutes les listes d'adresses associées à votre compte	List			
ListArchiveExports	Permet de répertorier toutes les exportations d'archives associées à votre compte	List			
ListArchiveSearches	Permet de répertorier toutes les recherches d'archives associées à votre compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListArchives	Permet de répertorier toutes les archives associées à votre compte	List			
ListIngressPoints	Permet de répertorier tous les points d'entrée associés à votre compte	List			
ListMembersOfAddressList	Accorde l'autorisation de répertorier tous les membres associés à une liste d'adresses	List	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListRelays	Permet de répertorier tous les relais SMTP associés à votre compte	List			
ListRuleSets	Accorde l'autorisation de répertorier tous les ensembles de règles associés à votre compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier tous les tags associés à la ressource	Lecture	addon-instance		
			addon-subscription		
			mailmanager-archive		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
ListTrafficPolicies	Permet de répertorier toutes les politiques de trafic associées à votre compte	List			
RegisterMemberToAddressList	Accorde l'autorisation d'ajouter un membre à une liste d'adresses	Écrire	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartAddressListImportJob	Accorde l'autorisation de démarrer une tâche d'importation sur une liste d'adresses	Écrire	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartArchiveExport	Autorise le lancement d'une exportation d'archives	Écrire	mailmanager-archive*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartArchiveSearch	Autorise le lancement d'une recherche dans les archives	Écrire	mailmanager-archive*		
StopAddressListImportJob	Autorise l'arrêt d'une tâche d'importation en cours sur une liste d'adresses	Écrire	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StopArchiveExport	Autorise l'arrêt de l'exportation des archives	Écrire	mailmanager-archive*		
StopArchiveSearch	Autorise l'arrêt de la recherche dans les archives	Écrire	mailmanager-archive*		
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises (clés et valeurs) à la ressource spécifiée	Balisage	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises (clés et valeurs) de la ressource spécifiée	Identification	addon-instance		
			addon-subscription		
			mailmanager-address-list		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			mailmanager-archive		
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys	
UpdateArchive	Accorde l'autorisation de mettre à jour une archive.	Écrire	mailmanager-archive*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateIngressPoint	Autorise la mise à jour d'un point d'entrée	Écrire	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey} ses:MailManagerTrafficPolicyArn ses:MailManagerRuleSetArn	
UpdateRelay	Autorise la mise à jour d'un relais SMTP	Écrire	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
UpdateRuleSet	Accorde l'autorisation de mettre à jour un ensemble de règles	Écrire	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTrafficPolicy	Autorise la mise à jour d'une politique de trafic	Écrire	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	

Types de ressources définis par Amazon Simple Email Service - Mail Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
addon-instance	`arn:${Partition}:ses:${Region}:${Account}:addon-instance/${AddonInstanceId}`	aws:ResourceTag/${TagKey}
addon-subscription	`arn:${Partition}:ses:${Region}:${Account}:addon-subscription/${AddonSubscriptionId}`	aws:ResourceTag/${TagKey}
mailmanager-archive	`arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
mailmanager-ingress-point	arn:${Partition}:ses:${Region}:${Account}:mailmanager-ingress-point/${IngressPointId}	aws:ResourceTag/${TagKey} ses:MailManagerIngressPointType
mailmanager-smtp-relay	arn:${Partition}:ses:${Region}:${Account}:mailmanager-smtp-relay/${RelayId}	aws:ResourceTag/${TagKey}
mailmanager-rule-set	arn:${Partition}:ses:${Region}:${Account}:mailmanager-rule-set/${RuleSetId}	aws:ResourceTag/${TagKey}
mailmanager-traffic-policy	arn:${Partition}:ses:${Region}:${Account}:mailmanager-traffic-policy/${TrafficPolicyId}	aws:ResourceTag/${TagKey}
mailmanager-address-list	arn:${Partition}:ses:${Region}:${Account}:mailmanager-address-list/${AddressListId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Simple Email Service - Mail Manager

Amazon Simple Email Service - Mail Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
ses:AddonSubscriptionArn	Filtre l'accès par l'ARN de l'abonnement à l'addon SES	ARN
ses:MailManagerIngressPointType	Filtre l'accès en fonction du type de point d'entrée de SES Mail Manager, par exemple OPEN ou AUTH	String
ses:MailManagerRuleSetArn	Filtre l'accès par l'ensemble de règles (ARN) de SES Mail Manager	ARN
ses:MailManagerTrafficPolicyArn	Filtre l'accès par la politique de trafic (ARN) de SES Mail Manager	ARN

Actions, ressources et clés de condition pour Amazon Simple Email Service v2

Amazon Simple Email Service V2 (préfixe de service : `ses`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Simple Email Service v2
- Types de ressources définis par Amazon Simple Email Service v2
- Clés de condition pour Amazon Simple Email Service v2

Actions définies par Amazon Simple Email Service v2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetMetricData	Accorde l'autorisation d'obtenir des données de métriques sur votre activité	Lecture	configuration-set		
			identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CancelExportJob	Accorde l'autorisation d'annuler une tâche d'exportation	Écrire	export-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion ses:ExportSourceType	
CreateConfigurationSet	Accorde l'autorisation de créer un ensemble de configurations	Écriture	configuration-set*		
			dedicated-ip-pool		
			mailmanager-archive		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Accorde l'autorisation de créer une destination d'événement d'ensemble de configurations	Écriture	configuration-set*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContact	Accorde l'autorisation de créer un contact	Écriture	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContactList	Accorde l'autorisation de créer une liste de contacts	Écriture	contact-list*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCustomVerificationEmailTemplate	Accorde l'autorisation de créer un nouveau modèle d'e-mail de vérification personnalisé	Écriture	custom-verification-email-template*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDedicatedIpPool	Accorde l'autorisation de créer un nouveau groupe d'adresses IP dédiées	Écriture	dedicated-ip-pool*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Accorde l'autorisation de créer un test prédictif de placement dans la boîte de réception	Écriture	identity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Accorde l'autorisation de démarrer un processus de vérification d'une identité d'adresse e-mail	Écriture	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentityPolicy	Accorde l'autorisation de créer la politique d'autorisation d'envoi spécifiée pour l'identité donnée	Gestion des autorisations	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Accorde l'autorisation de créer un modèle d'e-mail	Écrire	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportJob	Accorde l'autorisation de créer une tâche d'exportation	Écrire		ses:ApiVersion ses:ExportSourceType	
CreateImportJob	Accorde l'autorisation de créer une tâche d'importation pour une destination de données	Écrire		ses:ApiVersion	
CreateMultiRegionEndpoint	Accorde l'autorisation de créer un nouveau point de terminaison multirégional	Écrire		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateTenant	Accorde l'autorisation de créer un nouveau locataire	Écrire	tenant*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateTenantResourceAssociation	Accorde l'autorisation d'associer une ressource SES à un locataire	Écrire	configuration-set*		
			identity*		
			template*		
			tenant*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Accorde l'autorisation de supprimer un ensemble de configurations existant	Écriture	configuration-set*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Accorde l'autorisation de supprimer une destination d'événement	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContact	Accorde l'autorisation de supprimer un contact d'une liste de contacts	Écriture	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContactList	Accorde l'autorisation de supprimer une liste de contacts avec tous ses contacts	Écriture	contact-list*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteCustomVerificationEmailTemplate	Accorde l'autorisation de supprimer un modèle d'e-mail de vérification personnalisé existant	Écriture	custom-verification-email-template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Accorde l'autorisation de supprimer un groupe d'adresses IP dédié	Écriture	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Accorde l'autorisation de supprimer une identité d'e-mail	Écriture	identity*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentityPolicy	Accorde l'autorisation de supprimer la politique d'autorisation d'envoi spécifiée pour l'identité donnée (une adresse e-mail ou un domaine)	Gestion des autorisations	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailTemplate	Accorde l'autorisation de supprimer un modèle d'e-mail	Écrire	template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteMultiRegionEndpoint	Accorde l'autorisation de supprimer un point de terminaison multirégional	Écrire	multi-region-endpoint*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteSuppressedDestination	Accorde l'autorisation de supprimer une adresse e-mail de la liste de suppression de votre compte	Écrire		ses:ApiVersion	
DeleteTenant	Autorise la suppression d'un locataire	Écrire	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteTenantResourceAssociation	Accorde l'autorisation de supprimer une ressource SES associée à un locataire	Écrire	configuration-set*		
			identity*		
			template*		
			tenant*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Accorde l'autorisation d'obtenir des informations sur le statut et les fonctionnalités de l'envoi d'e-mail pour votre compte	Lecture		ses:ApiVersion	
GetBlacklistReports	Accorde l'autorisation de récupérer une liste des listes de refus sur lesquelles vos adresses IP dédiées ou vos domaines suivis apparaissent	Lecture		ses:ApiVersion	
GetConfigurationSet	Accorde l'autorisation d'obtenir des informations sur un ensemble de configurations existant	Lecture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConfigurationSetEventDestinations	Accorde l'autorisation de récupérer une liste des destinations d'événement qui sont associées à un ensemble de configurations	Lecture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContact	Accorde l'autorisation de renvoyer un contact d'une liste de contacts	Lecture	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContactList	Accorde l'autorisation de renvoyer des métadonnées d'une liste de contacts	Lecture	contact-list*		
				ses:ApiVersion	
GetCustomVerificationEmailTemplate	Accorde l'autorisation de renvoyer le modèle de vérification d'e-mail personnalisé pour le nom de modèle que vous spécifiez	Lecture	custom-verification-email-template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	Accorde l'autorisation d'obtenir des informations sur une adresse IP dédiée	Lecture		ses:ApiVersion	
GetDedicatedIpPool	Accorde l'autorisation d'obtenir des informations sur un pool d'IP dédié	Lecture	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIps	Accorde l'autorisation de répertorier les adresses IP dédiées vers un groupe d'adresses IP dédié	Lecture	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDeliverabilityDashboardOptions	Accorde l'autorisation d'obtenir le statut du tableau de bord de délivrabilité	Lecture		ses:ApiVersion	
GetDeliverabilityTestReport	Accorde l'autorisation de récupérer les résultats d'un test prédictif de placement dans la boîte de réception	Lecture	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Accorde l'autorisation de récupérer toutes les données de délivrabilité pour une campagne spécifique	Lecture		ses:ApiVersion	
GetDomainStatisticsReport	Accorde l'autorisation de récupérer des taux d'engagement et de placement de la boîte de réception pour les domaines que vous utilisez pour envoyer des e-mails	Lecture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailAddressInsights	Accorde l'autorisation d'obtenir des informations sur l'adresse e-mail	Lecture		ses:ApiVersion	iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEmailIdentity	Accorde l'autorisation d'obtenir des informations sur une identité spécifique	Lecture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentityPolicies	Accorde l'autorisation de renvoyer les stratégies d'autorisation d'envoi demandées pour l'identité donnée (une adresse e-mail ou un domaine)	Lecture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailTemplate	Accorde l'autorisation de renvoyer le modèle d'objet (qui comprend la ligne d'Objet, la partie HTML et la partie de texte) du modèle que vous spécifiez	Lecture	template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetExportJob	Accorde l'autorisation d'obtenir des informations sur une tâche d'exportation	Lecture	export-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion ses:ExportSourceType	
GetImportJob	Accorde l'autorisation de fournir des informations sur une tâche d'importation	Lecture	import-job*		
				ses:ApiVersion	
GetMessageInsights	Accorde l'autorisation de fournir des informations sur un message	Lecture		ses:ApiVersion	
GetMultiRegionEndpoint	Accorde l'autorisation d'obtenir des informations sur un point de terminaison multirégional	Lecture	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetReputationEntity	Accorde l'autorisation de récupérer des informations sur le statut d'une entité de réputation	Lecture	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetSuppressedDestination	Accorde l'autorisation de récupérer des informations sur une adresse e-mail spécifique figurant sur la liste de suppression de votre compte	Lecture		ses:ApiVersion	
GetTenant	Accorde l'autorisation d'obtenir des informations sur un locataire	Lecture	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Accorde l'autorisation de répertorier tous les ensembles de configurations pour votre compte	Liste		ses:ApiVersion	
ListContactLists	Accorde l'autorisation de répertorier toutes les listes de contacts disponibles pour votre compte	Liste		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListContacts	Accorde l'autorisation de répertorier les contacts présents dans une liste de contacts spécifique	Liste	contact-list*		
				ses:ApiVersion	
ListCustomVerificationEmailTemplates	Accorde l'autorisation de répertorier tous les modèles d'e-mail de vérification personnalisés existant pour votre compte	Liste		ses:ApiVersion	
ListDedicatedIpPools	Accorde l'autorisation de répertorier tous les groupes d'adresses IP dédiées pour votre compte	Liste		ses:ApiVersion	
ListDeliverabilityTestReports	AutoriAccorde l'autorisation de récupérer la liste des tests prédictifs de placement dans la boîte de réception que vous avez effectués, quel que soit leur statut, pour votre compte	Liste		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Accorde l'autorisation de répertorier des données de délivrabilité pour les campagnes ayant utilisé un domaine spécifique pour envoyer des e-mails pendant une période spécifiée	Lecture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEmailIdentities	Accorde l'autorisation de répertorier les identités d'e-mail de votre compte	Liste		ses:ApiVersion	
ListEmailTemplates	Accorde l'autorisation de répertorier tous les modèles d'e-mail de votre compte	List		ses:ApiVersion	
ListExportJobs	Accorde l'autorisation de répertorier toutes les tâches d'exportation de votre compte	List		ses:ApiVersion ses:ExportSourceType	
ListImportJobs	Accorde l'autorisation de répertorier toutes les tâches d'importation de votre compte	List		ses:ApiVersion	
ListMultiRegionEndpoints	Permet de répertorier tous les points de terminaison multirégionaux de votre compte	List		ses:ApiVersion	
ListRecommendations	Accorde l'autorisation de répertorier les recommandations pour votre compte	Lecture	identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListReputationEntities	Accorde l'autorisation de récupérer une liste d'entités de réputation	List	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListResourceTenants	Accorde l'autorisation de répertorier tous les locataires associés à une ressource SES	List	configuration-set*		
			identity*		
			template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListSuppressedDestinations	Accorde l'autorisation de répertorier des adresses e-mail figurant sur la liste de suppression de votre compte	Lecture		ses:ApiVersion	
ListTagsForResource	Accorde l'autorisation de récupérer une liste des balises (clés et valeurs) qui sont associées à une ressource spécifique pour votre compte	Lecture	configuration-set		
			contact-list		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		
				ses:ApiVersion	
ListTenantResources	Accorde l'autorisation de répertorier toutes les ressources associées à un locataire	List	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListTenants	Permet de répertorier tous les locataires de votre compte	List		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutAccountDedicatedIpWarmupAttributes	Accorde l'autorisation d'activer ou de désactiver la fonction de préparation automatique pour les adresses IP dédiées	Écriture		ses:ApiVersion	
PutAccountDetails	Accorde l'autorisation de mettre à jour les détails de votre compte	Écriture		ses:ApiVersion	
PutAccountSendingAttributes	Accorde l'autorisation d'activer ou de désactiver la possibilité pour votre compte d'envoyer des e-mails	Écriture		ses:ApiVersion	
PutAccountSuppressionAttributes	Accorde l'autorisation de modifier les paramètres de la liste de suppression au niveau du compte	Écrire		ses:ApiVersion	
PutAccountVdmAttributes	Accorde l'autorisation de modifier les paramètres de VDM pour votre compte	Écrire		ses:ApiVersion	
PutConfigurationSetArchivingOptions	Accorde l'autorisation d'associer un ensemble de configurations à une archive Mail Manager	Écrire	configuration-set*		
			mailmanager-archive		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetDeliveryOptions	Accorde l'autorisation d'association un ensemble de configurations à un groupe d'adresses IP dédiées	Écriture	configuration-set*		
			dedicated-ip-pool		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Accorde l'autorisation d'activer ou de désactiver la collecte des métriques de réputation pour les e-mails que vous envoyez à l'aide d'un ensemble de configurations	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutConfigurationSetSendingOptions	Accorde l'autorisation d'activer ou de désactiver l'envoi des messages qui utilisent un ensemble de configurations spécifique	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSuppressionOptions	Accorde l'autorisation de spécifier les préférences de liste de suppression de compte pour un ensemble de configurations particulier	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Accorde l'autorisation de spécifier un nom de domaine personnalisé à utiliser pour les éléments de suivi des ouvertures et des clics dans les e-mails que vous envoyez pour un ensemble de configurations spécifique	Écrire	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutConfigurationSetVdmOptions	Accorde l'autorisation de remplacer les paramètres de VDM au niveau du compte par un jeu de configurations particulier	Écrire	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Accorde l'autorisation de déplacer une adresse IP dédiée vers un groupe d'adresses IP dédiées existant	Écrire	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpPoolScalingAttributes	Accorde l'autorisation de transformer un groupe d'adresses IP dédiées standard en groupe géré.	Écrire	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Accorde l'autorisation de placer des attributs de mise en route IP dédiés	Écriture		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutDeliverabilityDashboardOption	Accorde l'autorisation d'activer ou de désactiver le tableau de bord de délivrabilité	Écriture		ses:ApiVersion	
PutEmailIdentityConfigurationSetAttributes	Accorde l'autorisation d'associer un ensemble de configurations à une identité e-mail	Écriture	identity* configuration-set	 ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimAttributes	Accorde l'autorisation d'activer ou de désactiver l'authentification DKIM pour une identité d'e-mail	Écriture	identity*	ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutEmailIdentityDkimSigningAttributes	Accorde l'autorisation de configurer ou de modifier les paramètres d'authentification DKIM pour une identité de domaine d'e-mail	Écriture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Accorde l'autorisation d'activer ou de désactiver le transfert de commentaires pour une identité d'e-mail	Écriture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Accorde l'autorisation d'activer ou de désactiver la configuration de domaine Mail-From personnalisée pour une identité d'e-mail	Écriture	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutSuppressedDestination	Accorde l'autorisation d'ajouter une adresse e-mail à la liste de suppression	Écrire		ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ReplicateEmailIdentityDkimSigningKey [autorisation uniquement]	Autorise la réplication de l'identité e-mail (clé de signature DKIM)	Gestion des autorisations	identity*		
				ses:ReplicaRegion	
SendBulkEmail	Accorde l'autorisation de composer un e-mail vers plusieurs destinations	Écriture	identity*		
			template*		
			configuration-set		
				ses:ApiVersion ses:MultiRegionEndpointId ses:TenantName	
SendCustomVerificationEmail	Accorde l'autorisation d'ajouter une adresse e-mail à la liste des identités et tente de la vérifier	Écriture	custom-verification-email-template*		
				ses:ApiVersion	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SendEmail	Accorde l'autorisation d'envoyer un e-mail	Écriture	identity*		
			configuration-set		
			template		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients ses:MultiRegionEndpointId ses:TenantName	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises (clés et valeurs) à la ressource spécifiée	Balisage	configuration-set		
			contact-list		
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TestRenderEmailTemplate	Accorde l'autorisation de créer un aperçu du contenu MIME d'un e-mail lorsqu'il est fourni avec un modèle et un jeu de données de remplacement	Écriture	template*		
				ses:ApiVersion	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises (clés et valeurs) de la ressource spécifiée	Balisage	configuration-set		
			contact-list		
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	Accorde l'autorisation de mettre à jour la configuration d'une destination d'événement pour un ensemble de configurations	Écriture	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContact	Accorde l'autorisation de mettre à jour les préférences d'un contact pour une liste	Écriture	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContactList	Accorde l'autorisation de mettre à jour des métadonnées de la liste de contacts	Écriture	contact-list*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateCustomVerificationEmailTemplate	Accorde l'autorisation de mettre à jour un modèle d'e-mail de vérification personnalisé existant	Écriture	custom-verification-email-template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailIdentityPolicy	Accorde l'autorisation de mettre à jour la politique d'autorisation d'envoi spécifiée pour l'identité donnée (une adresse e-mail ou un domaine)	Gestion des autorisations	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailTemplate	Accorde l'autorisation de mettre à jour un modèle d'e-mail	Écrire	template*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityCustomerManagedStatus	Accorde l'autorisation de mettre à jour le statut d'envoi géré par le client	Écrire	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityPolicy	Accorde l'autorisation d'attribuer une politique de réputation	Écrire	reputation-policy*		
			tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon Simple Email Service v2

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
reputation-policy	arn:${Partition}:ses:${Region}:aws:reputation-policy/${ReputationPolicyName}	
configuration-set	arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}	aws:ResourceTag/${TagKey}
contact-list	arn:${Partition}:ses:${Region}:${Account}:contact-list/${ContactListName}	aws:ResourceTag/${TagKey}
custom-verification-email-template	arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}	aws:ResourceTag/${TagKey}
dedicated-ip-pool	arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}	aws:ResourceTag/${TagKey}
deliverability-test-report	arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}	aws:ResourceTag/${TagKey}
export-job	arn:${Partition}:ses:${Region}:${Account}:export-job/${ExportJobId}	
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
import-job	arn:${Partition}:ses:${Region}:${Account}:import-job/${ImportJobId}	
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	aws:ResourceTag/${TagKey}
multi-region-endpoint	arn:${Partition}:ses:${Region}:${Account}:multi-region-endpoint/${EndpointName}	
mailmanager-archive	arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}	aws:ResourceTag/${TagKey}
tenant	arn:${Partition}:ses:${Region}:${Account}:tenant/${TenantName}/${TenantId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Simple Email Service v2

Amazon Simple Email Service V2 définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString
ses:ApiVersion	Filtre l'accès par la version de l'API SES	String
ses:ExportSourceType	Filtre l'accès par le type de source d'exportation	String
ses:FeedbackAddress	Filtre l'accès par l'adresse « Return-Path », qui spécifie l'adresse à laquelle les retours à l'expéditeur et les réclamations sont envoyés via le transfert de commentaires par e-mail	String
ses:FromAddress	Filtre l'accès par l'adresse « From » d'un message	String
ses:FromDisplayName	Filtre l'accès par l'adresse « From » utilisée comme nom d'affichage d'un message	String
ses:MultiRegionEndpointId	Filtre l'accès en fonction de l'ID de point de terminaison multirégional utilisé pour envoyer des e-mails	String
ses:Recipients	Filtre l'accès par les adresses des destinataires d'un message, qui incluent les adresses « To », « CC » et « BCC »	ArrayOfString
ses:ReplicaRegion	Filtre l'accès par régions de réplication pour la réplication de la clé de signature DKIM du domaine	ArrayOfString
ses:TenantName	Filtre l'accès en fonction du nom du locataire utilisé pour envoyer des e-mails	String

Actions, ressources et clés de condition pour Amazon Simple Workflow Service

Amazon Simple Workflow Service (préfixe de service : `swf`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les stratégies d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies pour Amazon Simple Workflow Service
- Types de ressources définis par Amazon Simple Workflow Service
- Clés de condition pour Amazon Simple Workflow Service

Actions définies pour Amazon Simple Workflow Service

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelTimer [autorisation uniquement]	Autorise l'annulation d'un chronomètre déjà lancé et l'enregistrement d'un TimerCanceled événement dans l'historique	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelWorkflowExecution [autorisation uniquement]	Accorde l'autorisation de fermer l'exécution du flux de travail et d'enregistrer un WorkflowExecutionCanceled événement dans l'historique	Écrire	domain*		
CompleteWorkflowExecution [autorisation uniquement]	Accorde l'autorisation de fermer l'exécution du flux de travail et d'enregistrer un WorkflowExecutionCompleted événement dans l'historique	Écrire	domain*		
ContinueAsNewWorkflowExecution [autorisation uniquement]	Accorde l'autorisation de fermer l'exécution du flux et de démarrer une nouvelle exécution de flux du même type à l'aide du même ID de flux et d'un ID d'exécution individuel.	Écrire	domain*		
CountClosedWorkflowExecutions	Accorde l'autorisation de renvoyer le nombre d'exécutions de flux fermées au sein du domaine donné qui répondent aux critères de filtre spécifiés.	Lecture	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CountOpenWorkflowExecutions	Accorde l'autorisation de renvoyer le nombre d'exécutions de flux ouvertes au sein du domaine donné qui répondent aux critères de filtre spécifiés.	Lecture	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountPendingActivityTasks	Accorde l'autorisation de renvoyer le nombre estimé de tâches d'activité dans la liste des tâches spécifiées.	Lecture	domain*		
				swf:taskList.name	
CountPendingDecisionTasks	Accorde l'autorisation de renvoyer le nombre estimé de tâches de décision dans la liste des tâches spécifiées.	Lecture	domain*		
				swf:taskList.name	
DeleteActivityType	Accorde l'autorisation de supprimer le type d'activité spécifié	Écrire	domain*		
				swf:activityType.name swf:activityType.version	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteWorkflowType	Accorde l'autorisation de supprimer le type de flux de travail spécifié	Écrire	domain*		
				swf:workflowType.name swf:workflowType.version	
DeprecateActivityType	Accorde l'autorisation de rendre obsolète le type d'activité spécifié.	Écrire	domain*		
				swf:activityType.name swf:activityType.version	
DeprecateDomain	Accorde l'autorisation de rendre obsolète le domaine spécifié.	Écrire	domain*		
DeprecateWorkflowType	Accorde l'autorisation de rendre obsolète le type de flux spécifié.	Écrire	domain*		
				swf:workflowType.name swf:workflowType.version	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeActivityType	Accorde l'autorisation de renvoyer des informations sur le type d'activité spécifié.	Lecture	domain*		
				swf:activityType.name swf:activityType.version	
DescribeDomain	Accorde l'autorisation de renvoyer des informations sur le domaine spécifié, y compris la description et l'état.	Lecture	domain*		
DescribeWorkflowExecution	Accorde l'autorisation de renvoyer des informations sur l'exécution du flux de travail spécifié, y compris son type et certaines statistiques.	Lecture	domain*		
DescribeWorkflowType	Accorde l'autorisation de renvoyer des informations sur le type de flux spécifié.	Lecture	domain*		
				swf:workflowType.name swf:workflowType.version	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
FailWorkflowExecution [autorisation uniquement]	Accorde l'autorisation de fermer l'exécution du flux de travail et d'enregistrer un WorkflowExecutionFailed événement dans l'historique	Écrire	domain*		
GetWorkflowExecutionHistory	Accorde l'autorisation de renvoyer l'historique de l'exécution de flux spécifié.	Lecture	domain*		
ListActivityTypes	Accorde l'autorisation de renvoyer des informations sur toutes les activités enregistrées dans le domaine spécifié qui correspondent au nom et à l'état d'enregistrement spécifiés.	List	domain*		
ListClosedWorkflowExecutions	Accorde l'autorisation de renvoyer une liste des exécutions de flux de travail fermées dans le domaine spécifié qui répondent aux critères de filtre.	List	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDomains	Accorde l'autorisation de renvoyer la liste des domaines enregistrés dans le compte.	List			
ListOpenWorkflowExecutions	Accorde l'autorisation de renvoyer une liste des exécutions de flux ouvertes dans le domaine spécifié qui répondent aux critères de filtre.	List	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une AWS ressource SWF	List	domain		
ListWorkflowTypes	Accorde l'autorisation de renvoyer des informations sur les types de flux dans le domaine spécifié.	List	domain*		
PollForActivityTask	Autorise les travailleurs à obtenir une ActivityTask TaskList à partir de l'activité spécifiée	Écrire	domain*		
				swf:taskList.name	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PollForDecisionTask	Accorde l'autorisation aux décideurs d'obtenir une TaskList DecisionTask à partir de la décision spécifiée	Écrire	domain*		
				swf:taskList.name	
RecordActivityTaskHeartbeat	Autorise les travailleurs à signaler au service que ActivityTask le TaskToken spécifié progresse toujours	Écrire	domain*		
RecordMarker [autorisation uniquement]	Autorise l'enregistrement d'un MarkerRecorded événement dans l'historique	Écrire	domain*		
RegisterActivityType	Accorde l'autorisation d'enregistrer un nouveau type d'activité ainsi que ses paramètres de configuration dans le domaine spécifié.	Écrire	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RegisterDomain	Accorde l'autorisation d'enregistrer un nouveau domaine.	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterWorkflowType	Accorde l'autorisation d'enregistrer un nouveau type de flux et ses paramètres de configuration dans le domaine spécifié.	Écrire	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask [autorisation uniquement]	Accorde l'autorisation de tenter d'annuler une tâche d'activité planifiée précédemment.	Écrire	domain*		
RequestCancelExternalWorkflowExecution [autorisation uniquement]	Accorde l'autorisation de demander qu'une requête soit envoyée pour annuler l'exécution du flux externe spécifié.	Écrire	domain*		
RequestCancelWorkflowExecution	Accorde l'autorisation d'enregistrer un WorkflowExecutionCancelRequested événement dans l'exécution du flux de travail en cours, identifié par le domaine, le WorkflowID et le RunID donnés	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RespondActivityTaskCanceled	Autorise les travailleurs à informer le service que le TaskToken ActivityTask identifié par le TaskToken a été annulé avec succès	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RespondActivityTaskCompleted	Autorise les travailleurs à indiquer au service que le TaskToken ActivityTask identifié par le TaskToken s'est terminé avec succès et a donné un résultat (s'il est fourni)	Écrire	domain*	swf:activityType.name swf:activityType.version swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				swf:workflowType.name swf:workflowType.version	
RespondActivityTaskFailed	Autorise les travailleurs à informer le service que le produit ActivityTask identifié par le TaskToken a échoué avec raison (si spécifié)	Écrire	domain*		
RespondDecisionTaskCompleted	Autorise les décideurs à indiquer au service que le service DecisionTask identifié par le TaskToken s'est terminé avec succès	Écrire	domain*		
ScheduleActivityTask [autorisation uniquement]	Accorde l'autorisation de planifier une tâche d'activité.	Écrire	domain*		
SignalExternalWorkflowExecution [autorisation uniquement]	Accorde l'autorisation de demander qu'un signal soit délivré à l'exécution et aux registres du flux externes spécifiés.	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SignalWorkflowExecution	Accorde l'autorisation d'enregistrer un WorkflowExecutionSignaled événement dans l'historique d'exécution du flux de travail et de créer une tâche de décision pour l'exécution du flux de travail identifiée par le domaine, le WorkflowID et le Runid donnés	Écrire	domain*		
StartChildWorkflowExecution [autorisation uniquement]	Accorde l'autorisation de demander le démarrage d'une exécution de flux enfant.	Écrire	domain*		
StartTimer [autorisation uniquement]	Accorde l'autorisation de démarrer l'exécution d'un minuteur pour un flux.	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartWorkflowExecution	Accorde l'autorisation de démarrer une exécution du type de flux dans le domaine spécifié à l'aide du workflowId et des données d'entrée fournis.	Écrire	domain*	swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name swf:workflowType.name swf:workflowType.version	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser une AWS ressource SWF	Identification	domain		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	Accorde l'autorisation d'enregistrer un WorkflowExecutionTerminated événement et de forcer la fermeture de l'exécution du flux de travail identifié par le domaine, le RunID et le WorkflowID donnés	Écrire	domain*		
UndeprecateActivityType	Accorde l'autorisation de rétablir un type d'activité précédemment rendu obsolète.	Écrire	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	Accorde l'autorisation de rétablir un domaine précédemment rendu obsolète.	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UndeprecateWorkflowType	Accorde l'autorisation de rétablir un type de flux précédemment rendu obsolète.	Écrire	domain*		
				swf:workflowType.name swf:workflowType.version	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource AWS SWF	Identification	domain		
				aws:TagKeys	

Types de ressources définis par Amazon Simple Workflow Service

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:swf::${Account}:/domain/${DomainName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Simple Workflow Service

Amazon Simple Workflow Service définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'étiquette de la requête.	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de l'étiquette de la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de l'étiquette de la clé.	ArrayOfString
swf:activityType.name	Filtre l'accès en fonction du nom du type d'activité.	String
swf:activityType.version	Filtre l'accès en fonction de la version du type d'activité.	String
swf:defaultTaskList.name	Filtre l'accès en fonction du nom de la liste de tâches par défaut.	String
swf:name	Filtre l'accès en fonction du nom des activités ou des flux.	String
swf:tagFilter.tag	Filtre l'accès en fonction de la valeur de tagFilter.tag.	String
swf:tagList.member.0	Filtre l'accès en fonction de l'étiquette spécifiée.	String
swf:tagList.member.1	Filtre l'accès en fonction de l'étiquette spécifiée.	String

Clés de condition	Description	Type
swf:tagList.member.2	Filtre l'accès en fonction de l'étiquette spécifiée.	String
swf:tagList.member.3	Filtre l'accès en fonction de l'étiquette spécifiée.	String
swf:tagList.member.4	Filtre l'accès en fonction de l'étiquette spécifiée.	String
swf:taskList.name	Filtre l'accès en fonction du nom de la liste des tâches.	String
swf:typeFilter.name	Filtre l'accès en fonction du nom du type de filtre.	String
swf:typeFilter.version	Filtre l'accès en fonction de la version du type de filtre.	String
swf:version	Filtre l'accès en fonction de la version des activités ou des flux.	String
swf:workflowType.name	Filtre l'accès en fonction du nom du type de flux.	String
swf:workflowType.version	Filtre l'accès en fonction de la version du type de flux.	String

Actions, ressources et clés de condition pour Amazon SimpleDB

Amazon SimpleDB (préfixe de service : `sdb`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon SimpleDB
- Types de ressources définis par Amazon SimpleDB
- Clés de condition pour Amazon SimpleDB

Actions définies par Amazon SimpleDB

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDeleteAttributes	Permet d'effectuer plusieurs DeleteAttributes opérations en un seul appel, ce qui réduit les allers-retours et les latences	Écrire	domain*		
BatchPutAttributes	Permet d'effectuer plusieurs PutAttribute opérations en un seul appel, ce qui réduit les allers-retours et les latences	Écrire	domain*		
CreateDomain	Accorde l'autorisation de créer un domaine	Écrire	domain*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAttributes	Accorde l'autorisation de supprimer un ou plusieurs attributs associés à l'élément	Écrire	domain*		
DeleteDomain	Accorde l'autorisation de supprimer un domaine	Écrire	domain*		
DomainMetadata	Accorde l'autorisation de renvoyer des informations sur le domaine, notamment la date de création du domaine, le nombre d'éléments et d'attributs, ainsi que la taille des noms et des valeurs des attributs	Lecture	domain*		
GetAttributes	Accorde l'autorisation de renvoyer tous les attributs associés à l'article	Lecture	domain*		
GetExport	Accorde l'autorisation de renvoyer des informations pour un domaine existant (ARN) d'exportation	Lecture	export*		
ListDomains	Accorde l'autorisation de répertorier tous les domaines	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListExports	Accorde l'autorisation de répertorier toutes les exportations créées. Les résultats sont paginés et peuvent être filtrés par nom de domaine	List	domain		
PutAttributes	Accorde l'autorisation de créer ou de remplacer des attributs dans un élément	Écrire	domain*		
Select	Accorde l'autorisation d'exécuter une requête sur les éléments d'un domaine	Lecture	domain*		
StartDomainExport	Accorde l'autorisation d'initier l'exportation d'un domaine SimpleDB vers un compartiment S3	Écrire	domain*		

Types de ressources définis par Amazon SimpleDB

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
domain	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}`	
export	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}/export/${ExportUUID}`	

Clés de condition pour Amazon SimpleDB

SimpleDB ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS SimSpace Weaver

AWS SimSpace Weaver (préfixe de service :`simspaceweaver`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS SimSpace Weaver
- Types de ressources définis par AWS SimSpace Weaver
- Clés de condition pour AWS SimSpace Weaver

Actions définies par AWS SimSpace Weaver

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSnapshot	Accorde l'autorisation de créer un instantané	Écrire	Simulation*		
DeleteApp	Accorde l'autorisation de supprimer une application	Écrire	Simulation*		
DeleteSimulation	Accorde l'autorisation de supprimer une simulation	Écrire	Simulation*		
DescribeApp	Accorde l'autorisation de décrire une application	Lecture	Simulation*		
DescribeSimulation	Accorde l'autorisation de décrire une simulation	Lecture	Simulation*		
ListApps	Accorde l'autorisation de répertorier les applications	Lecture	Simulation*		
ListSimulations	Accorde l'autorisation de répertorier les simulations	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartApp	Accorde l'autorisation de démarrer une application	Écrire	Simulation*		
StartClock	Accorde l'autorisation de démarrer une horloge de simulation	Écrire	Simulation*		
StartSimulation	Accorde l'autorisation de démarrer une simulation	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
StopApp	Accorde l'autorisation d'arrêter une application	Écrire	Simulation*		
StopClock	Accorde l'autorisation d'arrêter une horloge de simulation	Écrire	Simulation*		
StopSimulation	Accorde l'autorisation d'arrêter une simulation	Écrire	Simulation*		
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	Simulation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	Simulation*		
				aws:TagKeys	

Types de ressources définis par AWS SimSpace Weaver

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Simulation	`arn:${Partition}:simspaceweaver:${Region}:${Account}:simulation/${SimulationName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS SimSpace Weaver

AWS SimSpace Weaver définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour la gestion des appareils AWS Snow

AWS Snow Device Management (préfixe de service :`snow-device-management`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Snow Device Management
- Types de ressources définis par AWS Snow Device Management
- Clés de condition pour la gestion des équipements de AWS neige

Actions définies par AWS Snow Device Management

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelTask	Accorde l'autorisation d'annuler les tâches sur les appareils distants	Écrire	task*		
CreateTask	Accorde l'autorisation de créer des tâches sur des appareils distants	Écrire		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeDevice	Accorde l'autorisation de décrire un appareil géré à distance	Lecture	managed-device*		
DescribeDeviceEc2Instances	Accorde l'autorisation de décrire les instances EC2 d'un appareil géré à distance	Lecture	managed-device*		
DescribeExecution	Accorde l'autorisation de décrire les exécutions de tâches	Lecture			
DescribeTask	Accorde l'autorisation de décrire une tâche	Lecture	task*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDeviceResources	Accorde l'autorisation de répertorier les ressources d'un appareil géré à distance	List	managed-device*		
ListDevices	Accorde l'autorisation de répertorier les appareils gérés à distance	List			
ListExecutions	Accorde l'autorisation de répertorier les exécutions de tâches	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource (appareil ou tâche)	Lecture		aws:RequestTag/${TagKey} aws:TagKeys	
ListTasks	Accorde l'autorisation de répertorier les tâches	List			
TagResource	Accorde l'autorisation de baliser une ressource	Balisage	managed-device		
			task		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource	Identification	managed-device		
			task		
				aws:TagKeys	

Types de ressources définis par AWS Snow Device Management

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
managed-device	`arn:${Partition}:snow-device-management:${Region}:${Account}:managed-device/${ResourceId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:snow-device-management:${Region}:${Account}:task/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour la gestion des équipements de AWS neige

AWS Snow Device Management définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Snowball

AWS Snowball (préfixe de service :`snowball`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Snowball
- Types de ressources définis par AWS Snowball
- Clés de condition pour AWS Snowball

Actions définies par AWS Snowball

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelCluster	Octroie l'autorisation d'annuler une tâche de cluster	Écrire			
CancelJob	Octroie l'autorisation d'annuler la tâche spécifiée	Écrire			
CreateAddress	Octroie l'autorisation de créer une adresse vers laquelle envoyer un appareil Snowball	Écrire			
CreateCluster	Octroie l'autorisation de créer un cluster vide	Écrire			
CreateJob	Octroie l'autorisation de créer une tâche pour importer ou exporter des données entre Amazon S3 et votre centre de données sur site	Écrire			
CreateLongTermPricing	Accorde l'autorisation de créer une offre LongTermPricingListEntry permettant aux clients d'ajouter un contrat de facturation initiale pour une tâche	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateReturnShippingLabel	Accorde l'autorisation de créer une étiquette d'expédition qui sera utilisée pour renvoyer l'appareil Snow à AWS	Écrire			
DescribeAddress	Octroie l'autorisation d'obtenir des détails spécifiques sur cette adresse sous la forme d'un objet d'adresse	Lecture			
DescribeAddresses	Octroie l'autorisation de décrire un nombre spécifié d'objets d'ADRESSE	List			
DescribeCluster	Octroie l'autorisation de décrire les informations d'un cluster spécifique, y compris les informations d'expédition, le statut du cluster et d'autres métadonnées importantes	Lecture			
DescribeJob	Octroie l'autorisation de décrire les informations d'une tâche spécifique, y compris les informations d'expédition, le statut de la tâche et d'autres métadonnées importantes	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeReturnShippingLabel	Accorde l'autorisation de décrire les informations figurant sur l'étiquette d'expédition d'un appareil Snow retourné à AWS	Lecture			
GetJobManifest	Accorde l'autorisation d'obtenir un lien vers une URL présignée Amazon S3 pour le fichier manifeste associé à la valeur spécifiée JobId	Lecture			
GetJobUnlockCode	Accorde l'autorisation d'obtenir la valeur UnlockCode du code pour la tâche spécifiée	Lecture			
GetSnowballUsage	Octroie l'autorisation d'obtenir des informations sur la limite de service Snowball pour votre compte, ainsi que le nombre d'appareils Snowball que votre compte utilise	Lecture			
GetSoftwareUpdates	Accorde l'autorisation de renvoyer une URL présignée Amazon S3 pour un fichier de mise à jour associé à un JobId	Lecture			
ListClusterJobs	Accorde l'autorisation de répertorier JobListEntry les objets de la longueur spécifiée	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListClusters	Accorde l'autorisation de répertorier ClusterListEntry les objets de la longueur spécifiée	List			
ListCompatibleImages	Accorde l'autorisation de renvoyer une liste des différentes Amazon EC2 Amazon Machine Images (AMIs) qui vous appartiennent et Compte AWS qui pourraient être prises en charge pour une utilisation sur un appareil Snow	List			
ListJobs	Accorde l'autorisation de répertorier JobListEntry les objets de la longueur spécifiée	List			
ListLongTermPricing	Accorde l'autorisation de répertorier LongTermPricingListEntry des objets pour le compte qui fait la demande	Lecture			
ListPickupLocations	Accorde l'autorisation de répertorier les objets d'adresse pour lesquels le ramassage est disponible, de la longueur spécifiée	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceVersions	Octroie l'autorisation de répertorier toutes les versions prises en charge des services Snow sur appareil	List			
UpdateCluster	Accorde l'autorisation de mise à jour tant que la ClusterState valeur d'un cluster est dans l' AwaitingQuorum état, vous pouvez mettre à jour certaines des informations associées à un cluster	Écrire			
UpdateJob	Accorde l'autorisation de mise à jour tant que la JobState valeur d'une tâche est Nouvelle, vous pouvez mettre à jour certaines des informations associées à une tâche	Écrire			
UpdateJobShipmentState	Octroie l'autorisation de mettre à jour l'état d'expédition lorsque celui-ci change	Écrire			
UpdateLongTermPricing	Accorde l'autorisation de mettre à jour un contrat de facturation à l'avance spécifique pour une tâche	Écrire			

Types de ressources définis par AWS Snowball

AWS Snowball ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Snowball, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Snowball

Snowball ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon SNS

Amazon SNS (préfixe de service : `sns`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon SNS
- Types de ressources définis par Amazon SNS
- Clés de condition pour Amazon SNS

Actions définies par Amazon SNS

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddPermission	Accorde l'autorisation d'ajouter une déclaration à la politique de contrôle d'accès d'une rubrique, en accordant l'accès aux AWS comptes spécifiés aux actions spécifiées	Gestion des autorisations	topic*		
CheckIfPhoneNumberIsOptedOut	Accorde l'autorisation d'accepter un numéro de téléphone et d'indiquer si le titulaire du téléphone a refusé de recevoir des SMS provenant de votre compte.	Lecture			
ConfirmSubscription	Accorde l'autorisation de vérifier l'intention d'un propriétaire de point de terminaison de recevoir des messages en validant le jeton envoyé vers le point de terminaison par le biais d'une action d'abonnement précédente.	Écriture	topic*		
CreatePlatformApplication	Accorde l'autorisation de créer un objet d'application de plateforme pour l'un des services de notification push pris en charge, tels que APNS et GCM, auxquels les	Écriture			iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	appareils et les applications mobiles peuvent s'inscrire.				
CreatePlatformEndpoint	Accorde l'autorisation de créer un point de terminaison pour un appareil et une application mobile sur l'un des services de notification push pris en charge, comme GCM et APNS.	Écrire			
CreateSMSSandboxPhoneNumber	Accorde l'autorisation d'ajouter un numéro de téléphone de destination et d'envoyer un mot de passe à usage unique (OTP) à ce numéro de téléphone pour Compte AWS	Écrire			
CreateTopic	Accorde l'autorisation de créer une rubrique sur laquelle des notifications peuvent être publiées	Écriture	topic*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteEndpoint	Accorde l'autorisation de supprimer le point de terminaison pour un appareil et une application mobile d'Amazon SNS	Écriture			
DeletePlatformApplication	Accorde l'autorisation de supprimer un objet d'application de plateforme pour l'un des services de notification push pris en charge, comme APNS et GCM	Écrire			
DeleteSMSSandboxPhoneNumber	Accorde l'autorisation de supprimer le numéro Compte AWS de téléphone vérifié ou en attente d'un utilisateur	Écrire			
DeleteTopic	Accorde l'autorisation de supprimer une rubrique et tous ses abonnements	Écrire	topic*		
GetDataProtectionPolicy	Accorde l'autorisation de renvoyer la politique de protection des données d'une rubrique	Lecture	topic*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEndpointAttributes	Accorde l'autorisation de récupérer les attributs de point de terminaison pour un appareil sur l'un des services de notification push pris en charge, comme GCM et APNS.	Lecture			
GetPlatformApplicationAttributes	Accorde l'autorisation de récupérer les attributs de l'objet d'application de plateforme pour les services de notification push pris en charge, comme APNS et GCM.	Lecture			
GetSMSAttributes	Accorde l'autorisation de renvoyer les paramètres d'envoi de messages SMS à partir de votre compte	Lecture			
GetSMSSandboxAccountStatus	Accorde l'autorisation de récupérer l'état sandbox pour le compte appelant dans la région cible	Lecture			
GetSubscriptionAttributes	Accorde l'autorisation de renvoyer toutes les propriétés d'un abonnement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTopicAttributes	Accorde l'autorisation de renvoyer toutes les propriétés d'une rubrique	Lecture	topic*		
ListEndpointsByPlatformApplication	Accorde l'autorisation de répertorier les points de terminaison et leurs attributs pour des appareils dans un service de notification push pris en charge, comme GCM et APNS.	Liste			
ListOriginationNumbers	Accorde l'autorisation de répertorier tous les numéros d'origine et de leurs métadonnées	Liste			
ListPhoneNumbersOptedOut	Accorde l'autorisation de renvoyer une liste des numéros de téléphone qui sont désabonnés, ce qui signifie que vous ne pouvez pas leur envoyer de SMS	Lecture			
ListPlatformApplications	Accorde l'autorisation de répertorier les objets d'application de plateforme des services de notification push pris en charge, comme APNS et GCM.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSMSSandboxPhoneNumbers	Accorde l'autorisation de répertorier les numéros de téléphone de destination en attente et vérifiés du compte appelant	Liste			
ListSubscriptions	Accorde l'autorisation de renvoyer une liste des abonnements du demandeur	Liste			
ListSubscriptionsByTopic	Accorde l'autorisation de retourner la liste des abonnements à une rubrique spécifique.	Liste	topic*		
ListTagsForResource	Accorde l'autorisation de répertorier toutes les balises ajoutées à la rubrique Amazon SNS spécifiée	Lecture	topic		
ListTopics	Accorde l'autorisation de renvoyer une liste des sujets du demandeur	Liste			
OptInPhoneNumber	Accorde l'autorisation d'abonner un numéro de téléphone actuellement désabonné, ce qui vous permet de reprendre l'envoi de messages SMS à ce numéro.	Écriture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Publish	Accorde l'autorisation d'envoyer un message à tous les points de terminaison souscrits d'une rubrique	Écrire	topic*		
PutDataProtectionPolicy	Accorde l'autorisation de permettre à un propriétaire de rubrique de définir la politique de protection des données	Écrire	topic*		
RemovePermission	Accorde l'autorisation de supprimer une instruction de la politique de contrôle d'accès d'une rubrique	Gestion des autorisations	topic*		
SetEndpointAttributes	Accorde l'autorisation de définir les attributs d'un point de terminaison pour un appareil sur l'un des services de notification push pris en charge, comme GCM et APNS.	Écriture			
SetPlatformApplicationAttributes	Accorde l'autorisation de définir les attributs de l'objet d'application de plateforme pour les services de notification push pris en charge, comme APNS et GCM.	Écriture			iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetSMSAttributes	Accorde l'autorisation de définir les paramètres par défaut pour l'envoi de messages SMS et la réception de rapports quotidiens d'utilisation de SMS	Écriture			
SetSubscriptionAttributes	Autorise un propriétaire d'abonnement à définir une nouvelle valeur à un attribut de la rubrique	Écriture			
SetTopicAttributes	Autorise un propriétaire de rubrique à définir un attribut de la rubrique sur une nouvelle valeur	Gestion des autorisations	topic*		iam:PassRole
Subscribe	Accorde l'autorisation de se préparer à souscrire un point de terminaison en envoyant un message de confirmation au point de terminaison	Écriture	topic*		
				sns:Endpoint sns:Protocol	
TagResource	Accorde l'autorisation d'ajouter des balises à la rubrique Amazon SNS spécifiée	Balisage	topic		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Unsubscribe	Accorde l'autorisation de supprimer un abonnement	Écriture			
UntagResource	Accorde des autorisations pour supprimer les balises de la rubrique Amazon SNS	Identification	topic		
				aws:TagKeys	
VerifySMSSandboxPhoneNumber	Accorde l'autorisation de vérifier un numéro de téléphone de destination à l'aide d'un mot de passe à usage unique (OTP) pour un Compte AWS	Écrire			

Types de ressources définis par Amazon SNS

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon SNS

Amazon SNS définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès par les identifications de la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès par les clés d'identification à partir de la demande	ArrayOfString
sns:Endpoint	Filtre l'accès par l'URL, l'adresse e-email ou l'ARN provenant d'une demande d'abonnement ou d'un abonnement confirmé précédemment	String
sns:Protocol	Filtre l'accès par la valeur de protocole provenant d'une demande d'abonnement ou d'un abonnement confirmé précédemment	String

Actions, ressources et clés de condition pour AWS SQL Workbench

AWS SQL Workbench (préfixe de service :`sqlworkbench`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS SQL Workbench
- Types de ressources définis par AWS SQL Workbench
- Clés de condition pour AWS SQL Workbench

Actions définies par AWS SQL Workbench

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateConnectionWithChart [autorisation uniquement]	Accorde l'autorisation d'associer une connexion à un diagramme	Écrire	chart*		
			connection*		
AssociateConnectionWithTab [autorisation uniquement]	Accorde l'autorisation d'associer une connexion à un onglet	Écrire	connection*		
AssociateNotebookWithTab	Accorde l'autorisation d'associer un bloc-notes à un onglet	Écrire	notebook*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
AssociateQueryWithTab [autorisation uniquement]	Accorde l'autorisation d'associer une requête à un onglet	Écrire	query*		
BatchDeleteFolder [autorisation uniquement]	Accorde l'autorisation de supprimer des dossiers de votre compte	Écrire			
BatchGetNotebookCell [autorisation uniquement]	Accorde l'autorisation d'obtenir le contenu des cellules de bloc-notes dans votre compte	Lecture	notebook*		
CreateAccount [autorisation uniquement]	Accorde l'autorisation de créer un SQLWorkbench compte	Écrire			
CreateChart [autorisation uniquement]	Accorde l'autorisation de créer un graphique enregistré sur votre compte	Écrire	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConnection [autorisation uniquement]	Accorde l'autorisation de créer une connexion sur votre compte	Écrire	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFolder [autorisation uniquement]	Accorde l'autorisation de créer un dossier sur votre compte	Écrire			
CreateNotebook [autorisation uniquement]	Accorde l'autorisation de créer un nouveau bloc-notes dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookCell [autorisation uniquement]	Accorde l'autorisation de créer une cellule de bloc-notes dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateNotebookFromVersion [autorisation uniquement]	Accorde l'autorisation de créer un nouveau bloc-notes à partir d'une version de bloc-notes dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookVersion [autorisation uniquement]	Accorde l'autorisation de créer une version de bloc-notes dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSavedQuery [autorisation uniquement]	Accorde l'autorisation de créer une requête enregistrée sur votre compte	Écrire	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChart [autorisation uniquement]	Accorde l'autorisation de supprimer des graphiques sur votre compte	Écrire	chart*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteConnection [autorisation uniquement]	Accorde l'autorisation de supprimer des connexions sur votre compte	Écrire	connection*		
DeleteNotebook [autorisation uniquement]	Accorde l'autorisation de supprimer des blocs-notes dans votre compte	Écrire	notebook*		
DeleteNotebookCell [autorisation uniquement]	Accorde l'autorisation de supprimer des cellules de bloc-notes dans votre compte	Écrire	notebook*		
DeleteNotebookVersion [autorisation uniquement]	Accorde l'autorisation de supprimer des cellules de bloc-notes dans votre compte	Écrire	notebook*		
DeleteQCustomContext [autorisation uniquement]	Accorde l'autorisation de supprimer le contexte personnalisé à l'échelle du compte	Écrire			
DeleteSavedQuery [autorisation uniquement]	Accorde l'autorisation de supprimer des requêtes sur votre compte	Écrire	query*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSqlGenerationContext [autorisation uniquement]	Accorde l'autorisation de supprimer le contexte de génération SQL	Écrire			
DeleteTab [autorisation uniquement]	Accorde l'autorisation de supprimer un onglet sur votre compte	Écrire			
DriverExecute [autorisation uniquement]	Accorde l'autorisation d'exécuter une requête dans votre cluster redshift	Écrire	connection*		
DuplicateNotebook [autorisation uniquement]	Accorde l'autorisation de créer un nouveau bloc-notes en dupliquant un bloc-notes existant dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ExportNotebook [autorisation uniquement]	Accorde l'autorisation d'exporter un bloc-notes dans votre compte	Lecture	notebook*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GenerateSession [autorisation uniquement]	Accorde l'autorisation de générer une nouvelle session sur votre compte	Écrire			
GetAccountInfo [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations du compte	Lecture			
GetAccountSettings [autorisation uniquement]	Accorde l'autorisation d'obtenir les paramètres d'un compte	Lecture			
GetAutocompletionMetadata [autorisation uniquement]	Octroie l'autorisation d'obtenir les métadonnées de la structure de la base de données pour la saisie automatique.	Lecture			
GetAutocompletionResource [autorisation uniquement]	Octroie l'autorisation d'obtenir les informations de la structure de la base de données pour la saisie automatique.	Lecture			
GetChart [autorisation uniquement]	Accorde l'autorisation d'obtenir des graphiques sur votre compte	Lecture	chart*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConnection [autorisation uniquement]	Accorde l'autorisation d'obtenir des connexions sur votre compte	Lecture	connection*		
GetNotebook [autorisation uniquement]	Accorde l'autorisation d'obtenir les métadonnées de bloc-notes dans votre compte	Lecture	notebook*		
GetNotebookVersion [autorisation uniquement]	Accorde l'autorisation d'obtenir le contenu d'une version de bloc-notes dans votre compte	Lecture	notebook*		
GetQCustomContext [autorisation uniquement]	Accorde l'autorisation d'obtenir un contexte personnalisé à l'échelle du compte	Lecture			
GetQSqlPromptQuotas [autorisation uniquement]	Accorde l'autorisation d'obtenir un maximum de quotas d'invite SQL génératifs	Lecture			
GetQSqlRecommendations [autorisation uniquement]	Octroie l'autorisation d'obtenir des recommandations en texte vers SQL.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetQueryExecutionHistory [autorisation uniquement]	Accorde l'autorisation d'obtenir l'historique d'exécution des requêtes sur votre compte	Lecture			
GetSavedQuery [autorisation uniquement]	Accorde l'autorisation d'obtenir une requête enregistrée sur votre compte	Lecture	query*		
GetSchemaInference [autorisation uniquement]	Octroie l'autorisation d'obtenir les colonnes et les types de données à partir d'un fichier	Lecture			
GetSqlGenerationContext [autorisation uniquement]	Accorde l'autorisation d'obtenir le contexte de génération SQL	Lecture			
GetSqlRecommendations [autorisation uniquement]	Octroie l'autorisation d'obtenir des recommandations en texte vers SQL.	Lecture			
GetUserInfo [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations utilisateur	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetUserWorkspaceSettings [autorisation uniquement]	Accorde l'autorisation d'obtenir des paramètres d'espace de travail sur votre compte	Lecture			
ImportNotebook [autorisation uniquement]	Accorde l'autorisation d'importer un bloc-notes dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListConnections [autorisation uniquement]	Accorde l'autorisation de répertorier les connexions sur votre compte	List			
ListDatabases [autorisation uniquement]	Accorde l'autorisation de répertorier les bases de données de votre cluster redshift	List			
ListFiles [autorisation uniquement]	Accorde l'autorisation de répertorier les fichiers et dossiers	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNotebookVersions [autorisation uniquement]	Accorde l'autorisation d'obtenir les métadonnées de version de bloc-notes dans votre compte	List	notebook*		
ListNotebooks [autorisation uniquement]	Accorde l'autorisation de répertorier les blocs-notes dans votre compte	List			
ListQueryExecutionHistory [autorisation uniquement]	Accorde l'autorisation de répertorier l'historique d'exécution des requêtes sur votre compte	List			
ListRedshiftClusters [autorisation uniquement]	Accorde l'autorisation de répertorier les clusters redshift de votre compte	List			
ListSampleDatabases [autorisation uniquement]	Accorde l'autorisation de répertorier les exemples de base de données	Lecture			
ListSavedQueryVersions [autorisation uniquement]	Accorde l'autorisation de répertorier les versions d'une requête enregistrée sur votre compte	List	query*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTabs [autorisation uniquement]	Accorde l'autorisation de répertorier les onglets de votre compte.	List			
ListTaggedResources [autorisation uniquement]	Accorde l'autorisation de répertorier les ressources étiquetées	Lecture			
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation de répertorier les balises d'une ressource sqlworkbench	Lecture	chart		
			connection		
			notebook		
			query		
PassAccountSettings [autorisation uniquement]	Accorde l'autorisation de fournir les paramètres du compte avec la demande	Écrire			
PutQCustomContext [autorisation uniquement]	Accorde l'autorisation de mettre à jour le contexte personnalisé à l'échelle du compte	Écrire			
PutSqlGenerationContext [autorisation uniquement]	Accorde l'autorisation de mettre à jour le contexte de génération SQL	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutTab [autorisation uniquement]	Accorde l'autorisation de créer ou mettre à jour un onglet sur votre compte	Écrire			
PutUserWorkspaceSettings [autorisation uniquement]	Accorde l'autorisation de mettre à jour les paramètres d'espace de travail sur votre compte	Écrire			
RestoreNotebookVersion [autorisation uniquement]	Accorde l'autorisation de restaurer une version de bloc-notes dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [autorisation uniquement]	Accorde l'autorisation de baliser une ressource sqlworkbench	Identification	chart		
			connection		
			notebook		
			query		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation de supprimer la balise d'une ressource sqlworkbench	Identification	chart		
			connection		
			notebook		
			query		
				aws:TagKeys	
UpdateAccountConnectionSettings [autorisation uniquement]	Accorde l'autorisation de mettre à jour les paramètres de connexion à l'échelle d'un compte	Écrire			
UpdateAccountExportSettings [autorisation uniquement]	Accorde l'autorisation de mettre à jour les paramètres d'exportation à l'échelle d'un compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAccountGeneralSettings [autorisation uniquement]	Accorde l'autorisation de mettre à jour les paramètres généraux à l'échelle d'un compte	Écrire			
UpdateAccountQSqlSettings [autorisation uniquement]	Octroie l'autorisation de mettre à jour les paramètres en texte vers SQL à l'échelle d'un compte.	Écrire			
UpdateChart [autorisation uniquement]	Accorde l'autorisation de mettre à jour un graphique sur votre compte	Écrire	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateConnection [autorisation uniquement]	Accorde l'autorisation de mettre à jour une connexion sur votre compte	Écrire	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFileFolder [autorisation uniquement]	Accorde l'autorisation de déplacer des fichiers sur votre compte	Écrire	chart query		
UpdateFolder [autorisation uniquement]	Accorde l'autorisation de mise à jour le nom et les détails d'un dossier sur votre compte	Écrire			
UpdateNotebook [autorisation uniquement]	Accorde l'autorisation de mettre à jour les métadonnées de bloc-notes dans votre compte	Écrire	notebook* 	aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellContent [autorisation uniquement]	Accorde l'autorisation de mettre à jour le contenu d'une cellule de bloc-notes dans votre compte	Écrire	notebook* 	aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNotebookCellLayout [autorisation uniquement]	Accorde l'autorisation de mettre à jour la disposition des cellules de bloc-notes dans votre compte	Écrire	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateSavedQuery [autorisation uniquement]	Accorde l'autorisation de mettre à jour une requête enregistrée sur votre compte	Écrire	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Types de ressources définis par AWS SQL Workbench

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
connection	arn:${Partition}:sqlworkbench:${Region}:${Account}:connection/${ResourceId}	aws:ResourceTag/${TagKey}
query	arn:${Partition}:sqlworkbench:${Region}:${Account}:query/${ResourceId}	aws:ResourceTag/${TagKey}
chart	arn:${Partition}:sqlworkbench:${Region}:${Account}:chart/${ResourceId}	aws:ResourceTag/${TagKey}
notebook	arn:${Partition}:sqlworkbench:${Region}:${Account}:notebook/${ResourceId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS SQL Workbench

AWS SQL Workbench définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des étiquettes associées à la ressource	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon SQS

Amazon SQS (préfixe de service : `sqs`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon SQS
- Types de ressources définis par Amazon SQS
- Clés de condition pour Amazon SQS

Actions définies par Amazon SQS

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddPermission	Accorde une autorisation portant sur une file d'attente à un principal spécifique	Gestion des autorisations	queue*		
CancelMessageMoveTask	Accorde l'autorisation d'annuler une tâche de déplacement de messages en cours	Écrire	queue*		
ChangeMessageVisibility	Accorde l'autorisation de modifier le délai de visibilité d'un message spécifié dans une file d'attente avec une nouvelle valeur	Écrire	queue*		
CreateQueue	Accorde l'autorisation de créer une file d'attente ou renvoie l'URL d'une file d'attente existante	Écrire	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMessage	Accorde l'autorisation de supprimer le message spécifié de la file d'attente spécifiée	Écrire	queue*		
DeleteQueue	Accorde l'autorisation de supprimer la file d'attente	Écrire	queue*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	spécifiée par l'URL, que la file d'attente soit vide ou non				
GetQueueAttributes	Accorde l'autorisation d'obtenir des attributs pour la file d'attente spécifiée	Lecture	queue*		
GetQueueUrl	Accorde l'autorisation de renvoyer l'URL d'une file d'attente existante	Lecture	queue*		
ListDeadLetterSourceQueues	Accorde l'autorisation de renvoyer une liste de vos files d'attente dont l'attribut RedrivePolicy queue est configuré avec une file d'attente en lettres mortes	Lecture	queue*		
ListMessageMoveTasks	Accorde l'autorisation de répertorier les tâches de déplacement de messages	Lecture	queue*		
ListQueueTags	Accorde l'autorisation de répertorier les des balises ajoutées à une file d'attente SQS	Lecture	queue*		
ListQueues	Accorde l'autorisation de renvoyer une liste de vos files d'attente	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PurgeQueue	Accorde l'autorisation de supprimer les messages dans une file d'attente spécifiée par l'URL de file d'attente	Écrire	queue*		
ReceiveMessage	Accorde l'autorisation de récupérer un ou plusieurs messages, avec une limite maximale de 10 messages, à partir de la file d'attente spécifiée	Lecture	queue*		
RemovePermission	Accorde l'autorisation de révoquer toutes les autorisations de la politique de file d'attente qui correspond au paramètre Label spécifié	Gestion des autorisations	queue*		
SendMessage	Accorde l'autorisation de remettre un message dans la file d'attente spécifiée	Écrire	queue*		
SetQueueAttributes	Accorde l'autorisation de définir la valeur d'un ou plusieurs attributs de file d'attente	Écrire	queue*		
StartMessageMoveTask	Accorde l'autorisation de démarrer une tâche de déplacement de messages	Écrire	queue*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagQueue	Accorde l'autorisation d'ajouter des balises à la file d'attente SQS spécifiée	Identification	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagQueue	Accorde l'autorisation de supprimer des balises de la file d'attente SQS spécifiée	Identification	queue*		
				aws:TagKeys	

Types de ressources définis par Amazon SQS

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> L'ARN de la file d'attente est utilisé uniquement dans les stratégies d'autorisation IAM. Dans les appels d'API et de l'interface CLI, vous utilisez plutôt l'URL de la file d'attente.

Types de ressources	ARN	Clés de condition
queue	`arn:${Partition}:sqs:${Region}:${Account}:${QueueName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon SQS

Amazon SQS définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Step Functions

AWS Step Functions (préfixe de service :`states`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Step Functions
- Types de ressources définis par AWS Step Functions
- Clés de condition pour AWS Step Functions

Actions définies par AWS Step Functions

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateActivity	Accorde l'autorisation de créer une activité	Écriture	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachine	Accorde l'autorisation de créer une machine d'état	Écrire	statemachine*		iam:PassRole states:PublishStat

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					eMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachineAlias	Accorde l'autorisation de créer un alias de machine d'état	Écrire	statemachine*		
				states:StateMachineQualifier	
DeleteActivity	Accorde l'autorisation de supprimer une activité	Écriture	activity*		
DeleteStateMachine	Accorde l'autorisation de supprimer une machine d'état	Écrire	statemachine*		
DeleteStateMachineAlias	Accorde l'autorisation de supprimer un alias de machine d'état	Écrire	statemachine*		
				states:StateMachineQualifier	
DeleteStateMachineVersion	Accorde l'autorisation de supprimer une version de machine d'état	Écrire	statemachine*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				states:StateMachineQualifier	
DescribeActivity	Accorde l'autorisation de décrire une activité	Lecture	activity*		
DescribeExecution	Accorde l'autorisation de décrire une exécution	Lecture	execution*		
			express*		
DescribeMapRun	Accorde l'autorisation de décrire une exécution cartographique	Lecture	maprun*		
DescribeStateMachine	Accorde l'autorisation de décrire une machine d'état	Lecture	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineAlias	Accorde l'autorisation de décrire un alias de machine d'état	Lecture	statemachine*		
				states:StateMachineQualifier	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeStateMachineForExecution	Accorde l'autorisation de décrire la machine d'état d'une exécution	Lecture	execution*		
GetActivityTask	Autorise les employés à récupérer une tâche (avec l'ARN d'activité spécifié) dont l'exécution a été planifiée par une machine d'état en cours d'exécution	Écriture	activity*		
GetExecutionHistory	Accorde l'autorisation de renvoyer l'historique de l'exécution spécifiée sous la forme d'une liste d'événements	Lecture	execution*		
InvokeHTTPEndpoint [autorisation uniquement]	Octroie l'autorisation d'invoquer l'état de la tâche HTTP.	Écrire			
ListActivities	Accorde l'autorisation d'énumérer les activités existantes	Liste			
ListExecutions	Accorde l'autorisation de répertorier les exécutions d'une machine d'état	List	maprun*		
			statemachine*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				states:StateMachineQualifier	
ListMapRuns	Accorde l'autorisation de répertorier les exécutions cartographiques d'une exécution	List	execution*		
ListStateMachineAliases	Accorde l'autorisation de répertorier les alias d'une machine d'état	List	statemachine*		
				states:StateMachineQualifier	
ListStateMachineVersions	Accorde l'autorisation de répertorier les versions d'une machine d'état	List	statemachine*		
ListStateMachines	Accorde l'autorisation de répertorier les machines d'état existantes	List			
ListTagsForResource	Accorde l'autorisation de répertorier les tags d'une ressource AWS Step Functions	List	activity		
			statemachine		
PublishStateMachineVersion	Accorde l'autorisation de publier une version de machine d'état	Écrire	statemachine*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RedriveExecution	Accorde l'autorisation de rediriger une exécution	Écrire	execution*		
RevealSecrets [autorisation uniquement]	Octroie l'autorisation de révéler les données sensibles issues d'une exécution.	Lecture			
SendTaskFailure	Accorde l'autorisation de signaler l'échec de la tâche identifiée par taskToken	Écriture			
SendTaskHeartbeat	Accorde l'autorisation de signaler au service que la tâche représentée par taskToken spécifié est toujours en cours d'exécution	Écriture			
SendTaskSuccess	Accorde l'autorisation de signaler que la tâche identifiée par le taskToken s'est terminée avec succès	Écriture			
StartExecution	Accorde l'autorisation de démarrer l'exécution d'une machine d'état	Écriture	statemachine*		
				states:StateMachineQualifier	
StartSyncExecution	Accorde l'autorisation de démarrer une machine d'état Synchronous Express	Écriture	statemachine*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				states:StateMachineQualifier	
StopExecution	Accorde l'autorisation d'arrêter une exécution	Écrire	execution*		
TagResource	Accorde l'autorisation de baliser une ressource AWS Step Functions	Identification	activity		
			statemachine		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestState	Octroie l'autorisation de tester la définition d'une machine d'état.	Écrire			states:RevealSecrets
UntagResource	Accorde l'autorisation de supprimer un tag d'une ressource AWS Step Functions	Identification	activity		
			statemachine		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMapRun	Accorde l'autorisation de mettre à jour une exécution cartographique	Écrire	maprun*		
UpdateStateMachine	Accorde l'autorisation de mettre à jour une machine d'état	Écrire	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	Accorde l'autorisation de mettre à jour un alias de machine d'état	Écrire	statemachine*		
				states:StateMachineQualifier	
ValidateStateMachineDefinition	Accorde l'autorisation de valider une définition de machine à états	Lecture			

Types de ressources définis par AWS Step Functions

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
activity	`arn:${Partition}:states:${Region}:${Account}:activity:${ActivityName}`	aws:ResourceTag/${TagKey}
execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}:${ExecutionId}`	aws:ResourceTag/${TagKey}
express	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}:${ExecutionId}:${ExpressId}`	
statemachine	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}`	aws:ResourceTag/${TagKey}
statemachineversion	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineVersionId}`	aws:ResourceTag/${TagKey}
statemachinealias	`arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineAliasName}`	aws:ResourceTag/${TagKey}
maprun	`arn:${Partition}:states:${Region}:${Account}:mapRun:${StateMachineName}/${MapRunLabel}:${MapRunId}`	

Types de ressources	ARN	Clés de condition
labelled execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}/${MapRunLabel}:${ExecutionId}`	
labelled express	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}/${MapRunLabel}:${ExecutionId}:${ExpressId}`	

Clés de condition pour AWS Step Functions

AWS Step Functions définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString
states:HTTPEndpoint	Filtre l'accès par le point de terminaison autorisé par l'état de la tâche HTTP dans la demande.	String

Clés de condition	Description	Type
states:HTTPMethod	Filtre l'accès par la méthode autorisée par l'état de la tâche HTTP dans la demande.	String
states:StateMachineQualifier	Filtre l'accès en fonction du qualificateur d'un ARN de machine d'état	ArrayOfString

Actions, ressources et clés de condition pour AWS Storage Gateway

AWS Storage Gateway (préfixe de service :`storagegateway`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Storage Gateway
- Types de ressources définis par AWS Storage Gateway
- Clés de condition pour AWS Storage Gateway

Actions définies par AWS Storage Gateway

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateGateway	Accorde l'autorisation d'activer la passerelle que vous avez précédemment déployée sur votre hôte	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
AddCache	Accorde l'autorisation de configurer un ou plusieurs disques locaux de passerelle en tant que cache pour une passerelle à volume mis en cache	Écriture	gateway*		
AddTagsToResource	Accorde l'autorisation d'ajouter une ou plusieurs identifications à la ressource spécifiée	Balisage	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
AddUploadBuffer	Accorde l'autorisation de configurer un ou plusieurs disques locaux de passerelle en tant que tampon de chargement pour une passerelle spécifiée	Écriture	gateway*		
AddWorkingStorage	Accorde l'autorisation de configurer un ou plusieurs disques locaux de passerelle en tant que stockage de traitement pour une passerelle	Écriture	gateway*		
AssignTapePool	Accorde l'autorisation de déplacer une bande vers le groupe cible spécifié	Écrire	tape*		
			tapepool*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate FileSystem	Accorde l'autorisation d'associer un système de FSx fichiers Amazon à la passerelle de FSx fichiers Amazon	Écrire	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	Accorde l'autorisation de connecter un volume à une connexion iSCSI, puis attache le volume à la passerelle spécifiée	Écriture	gateway* volume*		
BypassGovernanceRetention	Accorde l'autorisation de contourner le verrou de rétention de gouvernance sur un groupe	Écriture	tapepool*		
CancelArchival	Accorde l'autorisation d'annuler l'archivage d'une bande virtuelle sur l'étagère de bandes virtuelles (VTS) après le démarrage du processus d'archivage	Écrire	gateway* tape*		
CancelCacheReport	Autorise l'annulation d'un rapport de cache	Écrire	cache-report*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelRetrieval	Accorde l'autorisation d'annuler la récupération d'une bande virtuelle à partir de l'étagère de bandes virtuelles (VTS) à destination d'une passerelle après le démarrage du processus de récupération	Écriture	gateway* tape*		
CreateCachediSCSIVolume	Accorde l'autorisation de créer un volume mis en cache sur une passerelle mise en cache spécifiée Cette opération est uniquement prise en charge pour l'architecture de volumes mis en cache sur la passerelle	Écriture	gateway* volume*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	Accorde l'autorisation de créer un partage de fichiers NFS sur une passerelle de fichiers existante	Écriture	gateway*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	Accorde l'autorisation de créer un partage de fichiers SMB sur une passerelle de fichiers existante	Écriture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Accorde l'autorisation de lancer un instantané d'un volume	Écriture	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotFromVolumeRecoveryPoint	Accorde l'autorisation de lancer un instantané d'une passerelle à partir d'un point de récupération de volume	Écriture	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	Accorde l'autorisation de créer un volume sur une passerelle spécifiée	Écriture	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTapePool	Accorde l'autorisation de créer un groupe de bandes	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	Accorde l'autorisation de créer une bande virtuelle à l'aide de votre propre code-barres	Écriture	gateway* tapepool*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapes	Accorde l'autorisation de créer une ou plusieurs bandes virtuelles. Vous écrivez des données sur les bandes virtuelles, puis vous archivez les bandes	Écriture	gateway* tapepool*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAutomaticTapeCreationPolicy	Accorde l'autorisation de supprimer la politique de création automatique de bandes configurée sur une passerelle VTL	Écriture	gateway*		
DeleteBandwidthRateLimit	Accorde l'autorisation de supprimer les limites de débit de bande passante d'une passerelle	Écrire	gateway*		
DeleteCacheReport	Accorde l'autorisation de supprimer les métadonnées associées à un rapport de cache	Écrire	cache-report*		
DeleteChapCredentials	Accorde l'autorisation de supprimer les informations d'identification via le protocole CHAP (Challenge-Handshake Authentication Protocol) pour une paire cible-initiateur iSCSI spécifiée	Écriture	target*		
DeleteFileShare	Accorde l'autorisation de supprimer un partage de fichiers à partir d'une passerelle de fichiers	Écriture	share*		
DeleteGateway	Accorde l'autorisation de supprimer une passerelle	Écriture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSnapshotSchedule	Accorde l'autorisation de supprimer un instantané d'un volume	Écriture	volume*		
DeleteTape	Accorde l'autorisation de supprimer la bande virtuelle spécifiée	Écriture	gateway*		
			tape*		
DeleteTapeArchive	Accorde l'autorisation de supprimer la bande virtuelle spécifiée de l'étagère de bandes virtuelles (VTS)	Écriture			
DeleteTapePool	Accorde l'autorisation de supprimer le groupe de bandes spécifié	Écrire	tapepool*		
DeleteVolume	Accorde l'autorisation de supprimer le volume de passerelle spécifié que vous avez créé précédemment à l'aide de l' CreateStorediSCSIVolume API CreateCachedi SCSIVolume or	Écrire	volume*		
DescribeAvailabilityMonitorTest	Accorde l'autorisation d'obtenir les informations sur le test de surveillance de haute disponibilité qui a été effectué le plus récemment sur la passerelle	Lecture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeBandwidthRateLimit	Accorde l'autorisation d'obtenir les limites de débit de bande passante d'une passerelle	Lecture	gateway*		
DescribeBandwidthRateLimitSchedule	Accorde l'autorisation d'obtenir le calendrier de limite de débit de bande passante d'une passerelle	Lecture	gateway*		
DescribeCache	Accorde l'autorisation d'obtenir des informations sur le cache d'une passerelle Cette opération est uniquement prise en charge pour l'architecture de volumes mis en cache sur la passerelle	Lecture	gateway*		
DescribeCacheReport	Accorde l'autorisation d'obtenir une description d'un rapport de cache	Lecture	cache-report*		
DescribeCachediSCSIVolumes	Accorde l'autorisation d'obtenir une description des volumes de passerelle spécifiés dans la requête. Cette opération est uniquement prise en charge pour l'architecture de volumes mis en cache sur la passerelle	Lecture	volume*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeChapCredentials	Accorde l'autorisation d'obtenir un tableau des informations d'identification via le protocole CHAP (Challenge-Handshake Authentication Protocol) pour une cible iSCSI spécifiée, une pour chaque paire cible-initiateur	Lecture	target*		
DescribeFileSystemAssociations	Accorde l'autorisation d'obtenir une description pour une ou plusieurs associations de systèmes de fichiers.	Lecture	fs-association*		
DescribeGatewayInformation	Accorde l'autorisation d'obtenir des métadonnées sur une passerelle telles que son nom, les interfaces réseau, le fuseau horaire configuré et son état (que la passerelle soit en cours d'exécution ou non)	Lecture	gateway*		
DescribeMaintenanceStartTime	Accorde l'autorisation d'obtenir l'heure de début de la maintenance hebdomadaire de votre passerelle, en particulier le jour et l'heure de la semaine	Lecture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeNFSFileShares	Accorde l'autorisation d'obtenir une description pour un ou plusieurs partages de fichiers à partir d'une passerelle de fichiers	Lecture	share*		
DescribeSMBFileShares	Accorde l'autorisation d'obtenir une description pour un ou plusieurs partages de fichiers à partir d'une passerelle de fichiers	Lecture	share*		
DescribeSMBSettings	Accorde l'autorisation d'obtenir une description des paramètres de partage de fichier SMB (Server Message Block) à partir d'une passerelle de fichiers	Lecture	gateway*		
DescribeSnapshotSchedule	Accorde l'autorisation de décrire le planning des instantanés pour le volume de passerelle spécifié	Lecture	volume*		
DescribeStorediSCSIVolumes	Accorde l'autorisation d'obtenir la description des volumes de passerelle spécifiés dans la demande	Lecture	volume*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTapeArchives	Accorde l'autorisation d'obtenir une description des bandes virtuelles spécifiées dans l'étagère de bandes virtuelles (VTS)	Lecture			
DescribeTapeRecoveryPoints	Accorde l'autorisation d'obtenir la liste des points de récupération de bandes virtuelles qui sont disponibles pour le dispositif Gateway-VTL spécifié	Lecture	gateway*		
DescribeTapes	Accorde l'autorisation d'obtenir une description de l'Amazon Resource Name (ARN) de bandes virtuelles	Lecture	gateway*		
DescribeUploadBuffer	Accorde l'autorisation d'obtenir des informations sur le tampon de chargement d'une passerelle	Lecture	gateway*		
DescribeVTLDevices	Accorde l'autorisation d'obtenir une description des périphériques de la bibliothèque de bandes virtuelles (VTL) pour la passerelle spécifiée	Lecture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWorkingStorage	Accorde l'autorisation d'obtenir des informations sur le stockage de traitement d'une passerelle	Lecture	gateway*		
DetachVolume	Accorde l'autorisation de se déconnecter d'un volume à partir d'une connexion iSCSI, puis détache le volume de la passerelle spécifiée	Écriture	volume*		
DisableGateway	Accorde l'autorisation de désactiver une passerelle lorsque la passerelle ne fonctionne plus	Écrire	gateway*		
DisassociateFileSystem	Accorde l'autorisation de dissocier un système de FSx fichiers Amazon d'une passerelle de FSx fichiers Amazon	Écrire	fs-association*		
EvictFilesFailingUpload	Accorde l'autorisation de nettoyer le cache d'un partage des entrées de fichiers dont le chargement sur Amazon S3 échoue	Écrire	share*		
JoinDomain	Accorde l'autorisation de vous permettre de rejoindre un domaine Active Directory	Écrire	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAutomaticTapeCreationPolicies	Permet de répertorier les politiques de création automatique de bandes configurées sur la passerelle VTL spécifiée ou sur toutes les passerelles appartenant à votre Compte AWS	List			
ListCacheReports	Accorde l'autorisation d'obtenir une liste des rapports de cache détenus par votre Compte AWS	List			
ListFileShares	Accorde l'autorisation d'obtenir la liste des partages de fichiers pour une passerelle de fichiers spécifique, ou la liste des partages de fichiers détenus par votre Compte AWS	List			
ListFileSystemAssociations	Accorde l'autorisation d'obtenir une liste des associations de systèmes de fichiers pour la passerelle spécifiée.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListGateways	Accorde l'autorisation de répertorier les passerelles détenues par et Compte AWS dans une région spécifiée dans la demande. La liste renvoyée est classée par Amazon Resource Name (ARN) de passerelle	Liste			
ListLocalDisks	Accorde l'autorisation d'obtenir une liste des disques locaux de la passerelle	Liste	gateway*		
ListTagsForResource	Accorde l'autorisation d'obtenir les identifications qui ont été ajoutées à la ressource spécifiée	List	gateway		
			share		
			tape		
			volume		
ListTapePools	Accorde l'autorisation de répertorier les pools de bandes appartenant à votre Compte AWS	List			
ListTapes	Accorde l'autorisation de répertorier des bandes virtuelles de votre bibliothèque de bandes virtuelles (VTL) et de votre étagère de bandes virtuelles (VTS)	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListVolumeInitiators	Accorde l'autorisation de répertorier des initiateurs iSCSI connectés à un volume	Liste	volume*		
ListVolumeRecoveryPoints	Accorde l'autorisation de répertorier les points de récupération pour une passerelle spécifiée	Liste	gateway*		
ListVolumes	Accorde l'autorisation de répertorier les volumes stockés iSCSI d'une passerelle	List			
NotifyWhenUploaded	Accorde l'autorisation de vous envoyer une notification via CloudWatch Events lorsque tous les fichiers écrits sur votre partage de fichiers NFS ont été chargés sur Amazon S3	Écrire	share*		
RefreshCache	Accorde l'autorisation d'actualiser le cache pour le partage de fichiers spécifié	Écriture	share*		
RemoveTagsFromResource	Accorde l'autorisation de supprimer une ou plusieurs identifications de la ressource spécifiée	Balisage	cache-report fs-association		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:TagKeys	
ResetCache	Accorde l'autorisation de réinitialiser tous les disques de mémoire cache qui ont rencontré une erreur et autorise la reconfiguration de ces disques en tant que stockages de cache	Écriture	gateway*		
RetrieveTapeArchive	Accorde l'autorisation de récupérer une bande virtuelle archivée de l'étagère de bandes virtuelles (VTS) vers une gateway-VTL	Écriture	gateway*		
			tape*		
RetrieveTapeRecoveryPoint	Accorde l'autorisation de récupérer le point de récupération de la bande virtuelle spécifiée	Écriture	gateway*		
			tape*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetLocalConsolePassword	Accorde l'autorisation de définir le mot de passe pour votre console locale de machine virtuelle	Écriture	gateway*		
SetSMBGuestPassword	Accorde l'autorisation de définir le mot de passe pour l'utilisateur invité SMB	Écriture	gateway*		
ShutdownGateway	Accorde l'autorisation d'arrêter une passerelle	Écriture	gateway*		
StartAvailabilityMonitorTest	Accorde l'autorisation de démarrer un test qui vérifie que la passerelle spécifiée est configurée pour la surveillance de la haute disponibilité dans votre environnement hôte	Écrire	gateway*		
StartCacheReport	Autorise le lancement d'un rapport de cache pour un partage de fichiers existant	Écrire	share*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartGateway	Accorde l'autorisation de démarrer une passerelle que vous avez précédemment arrêtée	Écriture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAutomaticTapeCreationPolicy	Accorde l'autorisation de mettre à jour la politique de création automatique de bande configurée sur une gateway-VTL	Écriture	gateway* tapepool*		
UpdateBandwidthRateLimit	Accorde l'autorisation de mettre à jour les limites de débit de bande passante d'une passerelle	Écriture	gateway*		
UpdateBandwidthRateLimitSchedule	Accorde l'autorisation de mettre à jour le calendrier de limite de débit de bande passante d'une passerelle	Écriture	gateway*		
UpdateChapCredentials	Accorde l'autorisation de mettre à jour les informations d'identification via le protocole CHAP (Challenge-Handshake Authentication Protocol) pour une cible iSCSI spécifiée	Écriture	target*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateFileSystemAssociation	Accorde l'autorisation de mettre à jour une association de système de fichiers.	Écriture	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
UpdateGatewayInformation	Accorde l'autorisation de mettre à jour les métadonnées d'une passerelle, ce qui inclut le nom et le fuseau horaire de la passerelle	Écriture	gateway*		
UpdateGatewaySoftwareNow	Accorde l'autorisation de mettre à jour le logiciel de la machine virtuelle (VM) de passerelle	Écriture	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMaintenanceStartTime	Accorde l'autorisation demettre à jour l'heure de début de la maintenance hebdomadaire d'une passerelle, en particulier le jour et l'heure de la semaine. L'heure de maintenance est l'heure dans le fuseau horaire de votre passerelle	Écriture	gateway*		
UpdateNFSFileShare	Accorde l'autorisation de mettre à jour un partage de fichiers NFS	Écriture	share*		
UpdateSMBFileShare	Accorde l'autorisation de mettre à jour un partage de fichiers SMB	Écriture	share*		
UpdateSMBFileShareVisibility	Accorde l'autorisation de mettre à jour la visibilité des partages d'une passerelle dans une vue réseau ou dans une liste de navigation	Écrire	gateway*		
UpdateSMBLocalGroups	Accorde l'autorisation de mettre à jour la liste des utilisateurs et groupes Active Directory disposant d'autorisations spéciales pour les partages de fichiers SMB sur la passerelle	Écrire	gateway*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSMBSecurityStrategy	Accorde l'autorisation de mettre à jour la stratégie de sécurité SMB sur une passerelle de fichiers	Écriture	gateway*		
UpdateSnapshotSchedule	Accorde l'autorisation de mettre à jour une planification d'instantanés configuré pour un volume de passerelle	Écriture	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	Accorde l'autorisation de mettre à jour le type de changement de support dans une gateway-VTL	Écrire	device*		

Types de ressources définis par AWS Storage Gateway

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
cache-report	arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}/cache-report/${CacheReportId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/device/${Vtldevice}	
fs-association	arn:${Partition}:storagegateway:${Region}:${Account}:fs-association/${FsaId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
share	arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}	aws:ResourceTag/${TagKey}
tape	arn:${Partition}:storagegateway:${Region}:${Account}:tape/${TapeBarcode}	aws:ResourceTag/${TagKey}
tapepool	arn:${Partition}:storagegateway:${Region}:${Account}:tapepool/${PoolId}	aws:ResourceTag/${TagKey}
target	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/target/${IscsiTarget}	
volume	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/volume/${VolumeId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Storage Gateway

AWS Storage Gateway définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour la chaîne AWS d'approvisionnement

AWS La chaîne d'approvisionnement (préfixe de service :`scn`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par la chaîne AWS d'approvisionnement

- Types de ressources définis par la chaîne AWS d'approvisionnement
- Clés de condition pour la chaîne AWS d'approvisionnement

Actions définies par la chaîne AWS d'approvisionnement

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssignAdminPermissionsToUser	Accorde l'autorisation d'ajouter l'autorisation d'administrateur de la chaîne d' AWS approvisionnement à un utilisateur fédéré	Écrire	instance*		
CreateBillOfMaterialsImportJob	Accorde l'autorisation de créer un fichier BillOfMaterialsImportJob qui importera un fichier CSV d' BillOfMaterials enregistrements	Écrire	instance*		
CreateDataIntegrationFlow	Accorde l'autorisation de créer une solution DataIntegrationFlow capable de transformer plusieurs sources en une seule cible	Écrire	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataLakeDataset	Accorde l'autorisation de créer le jeu de données du lac de données	Écrire	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeNamespace	Accorde l'autorisation de créer l'espace de noms du lac de données	Écrire	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInstance	Accorde l'autorisation de créer une nouvelle instance AWS de chaîne d'approvisionnement	Écrire	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSSOApplication	Accorde l'autorisation de créer une application IAM Identity Center pour une instance de chaîne AWS d'approvisionnement	Écrire	instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteDataIntegrationFlow	Accorde l'autorisation de supprimer le DataIntegrationFlow	Écrire	data-integration-flow*		
DeleteDataLakeDataset	Accorde l'autorisation de supprimer le jeu de données du lac de données	Écrire	dataset*		
DeleteDataLakeNamespace	Autorise la suppression de l'espace de noms du lac de données	Écrire	namespace*		
DeleteInstance	Accorde l'autorisation de supprimer une instance AWS de chaîne d'approvisionnement	Écrire	instance*		
DeleteSSOApplication	Autorise la suppression de l'application IAM Identity Center de l'instance AWS Supply Chain	Écrire	instance*		
DescribeInstance	Accorde l'autorisation d'afficher les détails d'une instance de chaîne AWS d'approvisionnement	Lecture	instance*		
GetBillOfMaterialsImportJob	Accorde l'autorisation de consulter le statut et les détails d'un BillOfMaterialsImportJob	Lecture	bill-of-materials-import-job*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDataIntegrationEvent	Accorde l'autorisation d'obtenir un DataIntegrationEvent	Lecture	instance*		
GetDataIntegrationFlow	Accorde l'autorisation d'obtenir les DataIntegrationFlow détails	Lecture	data-integration-flow*		
GetDataIntegrationFlowExecution	Accorde l'autorisation d'obtenir une exécution particulière d'une exécution spécifiée DataIntegrationFlow	Lecture	data-integration-flow*		
GetDataLakeDataset	Accorde l'autorisation d'obtenir les détails du jeu de données	Lecture	dataset*		
GetDataLakeNamespace	Accorde l'autorisation d'obtenir les détails de l'espace de noms	Lecture	namespace*		
GetInstance	Accorde l'autorisation d'afficher les détails d'une instance de chaîne AWS d'approvisionnement	Lecture	instance*		
ListAdminUsers	Accorde l'autorisation de répertorier les administrateurs de la chaîne d' AWS approvisionnement d'une instance	List	instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDataIntegrationEvents	Accorde l'autorisation de tout répertorier DataIntegrationEvents sous une instance	List	instance*		
ListDataIntegrationFlowExecutions	Accorde l'autorisation de répertorier toutes les exécutions d'une exécution spécifiée DataIntegrationFlow	List	data-integration-flow*		
ListDataIntegrationFlows	Accorde l'autorisation de tout répertorier de DataIntegrationFlows manière paginée	List	instance*		
ListDataLakeDatasets	Accorde l'autorisation de répertorier les ensembles de données du lac de données sous une instance ou un espace de noms spécifique	List	instance*		
ListDataLakeNamespaces	Accorde l'autorisation de répertorier les espaces de noms du lac de données sous une instance spécifique	List	instance*		
ListInstances	Accorde l'autorisation de consulter les instances AWS de la chaîne d'approvisionnement associées à un Compte AWS	List	instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour une ressource AWS de la chaîne d'approvisionnement	List	instance*		
RemoveAdminPermissionsForUser	Accorde l'autorisation de supprimer l'autorisation d'administrateur de la chaîne d' AWS approvisionnement à un utilisateur fédéré	Écrire	instance*		
SendDataIntegrationEvent	Autorise la création d'un fichier DataIntegrationEvent qui ingérera des données en temps réel	Écrire	instance*		
TagResource	Accorde l'autorisation de baliser une ressource AWS de la chaîne d'approvisionnement	Identification	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer le tag d'une ressource de la chaîne AWS d'approvisionnement	Identification	instance*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDataIntegrationFlow	Accorde l'autorisation de mettre à jour le DataIntegrationFlow	Écrire	data-integration-flow*		
UpdateDataLakeDataset	Autorise la mise à jour du jeu de données du lac de données	Écrire	dataset*		
UpdateDataLakeNamespace	Autorise la mise à jour de l'espace de noms du lac de données	Écrire	namespace*		
UpdateInstance	Autorise la mise à jour d'une instance AWS de chaîne d'approvisionnement	Écrire	instance*		

Types de ressources définis par la chaîne AWS d'approvisionnement

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
instance	`arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
bill-of-materials-import-job	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/bill-of-materials-import-job/${JobId}	
data-integration-flow	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/data-integration-flows/${FlowName}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}/datasets/${DatasetName}	aws:ResourceTag/${TagKey}

Clés de condition pour la chaîne AWS d'approvisionnement

AWS La chaîne d'approvisionnement définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification dans la requête	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans la requête	ArrayOfString

Actions, ressources et clés de condition pour AWS Support

AWS Support (préfixe de service :`support`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Support
- Types de ressources définis par AWS Support
- Clés de condition pour AWS Support

Actions définies par AWS Support

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> Support permet d'accéder aux cas, de les modifier et de les résoudre, ainsi que d'utiliser les actions Trusted Advisor. Lorsque vous utilisez l'API Support pour appeler des actions liées à

Trusted Advisor, aucune des actions « trustedadvisor:* » ne limite votre accès. Les actions « trustedadvisor:* » s'appliquent uniquement à Trusted Advisor dans la AWS Management Console.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AddAttachmentsToSet	Accorde l'autorisation d'ajouter une ou plusieurs pièces jointes à un AWS Support dossier	Écrire			
AddCommunicationToCase	Accorde l'autorisation d'ajouter une communication client à un AWS Support dossier	Écrire			
CreateCase	Accorde l'autorisation de créer un nouveau AWS Support dossier	Écrire			
DescribeAttachment	Accorde l'autorisation de décrire les détails des pièces jointes	Lecture			
DescribeCaseAttributes	Accorde l'autorisation d'autoriser les services secondaires à lire les attributs des AWS Support dossiers. Il s'agit d'une fonction gérée en interne	Lecture			
DescribeCaseOptions	Accorde l'autorisation de décrire les options disponibles pour un seul AWS Support	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	cas. Il s'agit d'une fonction gérée en interne				
DescribeCases	Accorde l'autorisation de répertorier les AWS Support cas qui correspondent aux entrées données	Lecture			
DescribeCommunication	Accorde l'autorisation d'obtenir une communication et des pièces jointes uniques pour un seul AWS Support cas	Lecture			
DescribeCommunications	Accorde l'autorisation de répertorier les communications et les pièces jointes pour un ou plusieurs AWS Support cas	Lecture			
DescribeCreateCaseOptions	Accorde l'autorisation de décrire les options disponibles pour créer un cas d'assistance	Lecture			
DescribeIssueTypes	Accorde l'autorisation de renvoyer les types de problèmes pour les AWS Support dossiers	Lecture			
DescribeServices	Accorde l'autorisation de répertorier les AWS services et les catégories applicables à chaque service	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSeverityLevels	Accorde l'autorisation de répertorier les niveaux de gravité pouvant être attribués à un AWS Support cas	Lecture			
DescribeSupportLevel	Accorde l'autorisation de renvoyer le niveau de support pour un identifiant de AWS compte	Lecture			
DescribeSupportedLanguages	Accorde l'autorisation de décrire les langues d'assistance disponibles pour un code de catégorie, un code de service et un type de problème donnés	Lecture			
DescribeTrustedAdvisorCheckRefreshStatuses	Accorde l'autorisation d'obtenir l'état d'une vérification d'actualisation de Trusted Advisor basée sur une liste d'identificateurs de vérification	Lecture			
DescribeTrustedAdvisorCheckResult	Accorde l'autorisation d'obtenir les résultats de la vérification Trusted Advisor qui correspond à l'identificateur de vérification spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeTrustedAdvisorCheckSummaries	Accorde l'autorisation d'obtenir les résumés des résultats des vérifications Trusted Advisor qui correspondent aux identificateurs de vérification spécifiés	Lecture			
DescribeTrustedAdvisorChecks	Accorde l'autorisation d'obtenir une liste de toutes les vérifications Trusted Advisor disponibles, y compris le nom, l'identificateur, la catégorie et la description	Lecture			
GetInteraction	Accorde l'autorisation de bénéficier d'une assistance personnalisée en cas de problème de compte et de problèmes techniques liés à une interaction spécifique	Lecture			
InitiateCallForCase	Accorde l'autorisation de lancer un appel au AWS Support Centre. Il s'agit d'une fonction gérée en interne	Écrire			
InitiateChatForCase	Accorde l'autorisation d'initier une discussion sur AWS Support Center.Il s'agit d'une fonction gérée en interne	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
InitiateLiveContactForCase	Accorde l'autorisation d'établir un contact en direct sur AWS Support Center. Il s'agit d'une fonction gérée en interne	Écrire			
ListInteractionEntries	Accorde l'autorisation de récupérer une liste d'entrées dans le cadre d'une interaction spécifique, y compris des messages, des mises à jour de statut ou d'autres points de données pertinents	Lecture			
ListInteractions	Accorde l'autorisation de récupérer une liste d'interactions, éventuellement à l'aide de filtres ou de pagination	Lecture			
PutCaseAttributes	Accorde l'autorisation d'autoriser les services secondaires à associer des attributs aux AWS Support dossiers. Il s'agit d'une fonction gérée en interne	Écrire			
RateCaseCommunication	Autorise l'évaluation d'une communication relative à un AWS Support dossier	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RefreshTrustedAdvisorCheck	Accorde l'autorisation de demander une actualisation de la vérification Trusted Advisor correspondant à l'identificateur de vérification spécifié	Écrire			
ResolveCase	Accorde l'autorisation de résoudre un AWS Support cas	Écrire			
ResolveInteraction	Accorde l'autorisation de marquer une interaction spécifique comme étant résolue par son identifiant unique, indiquant que le problème a été résolu et qu'aucune autre action n'est nécessaire	Écrire			
SearchForCases	Accorde l'autorisation de renvoyer une liste de AWS Support cas correspondant aux entrées données	Lecture			
StartInteraction	Accorde l'autorisation de démarrer une interaction spécifique afin de bénéficier d'une assistance personnalisée en cas de problème technique ou lié au compte	Écrire			support:DescribeSupportLevel

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCaseSeverity	Accorde l'autorisation de mettre à jour la gravité d'un seul AWS Support cas. Il s'agit d'une fonction gérée en interne	Écrire			
UpdateInteraction	Autorise la mise à jour d'une interaction spécifique afin de bénéficier d'une assistance personnalisée en cas de problème technique ou lié au compte	Écrire			

Types de ressources définis par AWS Support

AWS Support ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Support, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Support

Support ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour une AWS Support application dans Slack

AWS Support Dans Slack, l'application (préfixe de service :`supportapp`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Support l'application dans Slack
- Types de ressources définis par AWS Support l'application dans Slack
- Clés de condition pour AWS Support l'application dans Slack

Actions définies par AWS Support l'application dans Slack

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSlackChannelConfiguration	Accorde l'autorisation de créer une configuration de canal Slack pour votre compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccountAlias	Accorde l'autorisation de supprimer un alias de votre compte	Écrire			
DeleteSlackChannelConfiguration	Accorde l'autorisation de supprimer une configuration de canal Slack de votre compte	Écrire			
DeleteSlackWorkspaceConfiguration	Accorde l'autorisation de supprimer une configuration d'espace de travail Slack de votre compte	Écrire			
DescribeSlackChannels [autorisation uniquement]	Permet de répertorier toutes les chaînes Slack publiques d'un espace de travail qui ont invité l'application AWS Support	Lecture			
GetAccountAlias	Accorde l'autorisation d’obtenir un alias pour votre compte	Lecture			
GetSlackOauthParameters [autorisation uniquement]	Accorde l'autorisation d'obtenir les paramètres du OAuth code Slack, que l' AWS Support application utilise pour autoriser l'espace de travail	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSlackChannelConfigurations	Accorde l'autorisation de répertorier toutes les configurations de canal Slack pour votre compte	Lecture			
ListSlackWorkspaceConfigurations	Accorde l'autorisation de répertorier toutes les configurations d'espace de travail pour votre compte	Lecture			
PutAccountAlias	Accorde l'autorisation de créer ou de mettre à jour un alias pour votre compte	Écrire			
RedeemSlackOauthCode [autorisation uniquement]	Accorde l'autorisation d'utiliser le OAuth code Slack, que l' AWS Support application utilise pour autoriser l'espace de travail	Écrire			
RegisterSlackWorkspaceForOrganization	Accorde l'autorisation d'enregistrer un espace de travail Slack pour un Compte AWS membre d'une organisation	Écrire			
UpdateSlackChannelConfiguration	Accorde l'autorisation de mettre à jour une configuration de canal Slack pour votre compte	Écrire			

Types de ressources définis par AWS Support l'application dans Slack

AWS Support Dans Slack, l'application ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à l'application AWS Support dans Slack, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Support l'application dans Slack

L'application prise en charge ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Support la console

AWS Support La console (préfixe de service :`support-console`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Support la console
- Types de ressources définis par AWS Support la console
- Clés de condition pour AWS Support console

Actions définies par AWS Support la console

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CheckSubscription [autorisation uniquement]	Accorde l'autorisation de vérifier si le compte a accès au produit donné	Lecture			
CreateCaseDraft [autorisation uniquement]	Accorde l'autorisation de créer ou de mettre à jour un brouillon de dossier pour le type de dossier donné	Écrire			
CreateContact [autorisation uniquement]	Accorde l'autorisation de créer un contact authentifié pour le type de contact donné	Écrire			
DeleteCaseDraft [autorisation uniquement]	Autorise la suppression d'une ébauche de dossier pour le type de dossier donné	Écrire			
DescribeDynamicHelp [autorisation uniquement]	Autorise l'accès à des ressources d'aide dynamiques pour un service ou une catégorie donnés	Lecture			
GetAccountGovCloudEnabled [autorisation uniquement]	Accorde l'autorisation de déterminer si le compte d'appel est GovCloud activé	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountState [autorisation uniquement]	Accorde l'autorisation d'obtenir l'état du compte d'appel	Lecture			
GetBanner [autorisation uniquement]	Accorde l'autorisation d'obtenir les informations de la bannière d'assistance	Lecture			
GetCaseDraft [autorisation uniquement]	Accorde l'autorisation d'obtenir un brouillon pour un type de cas donné	Lecture			
GetIssueClassificationPredictions [autorisation uniquement]	Accorde l'autorisation d'obtenir les prédictions de classification d'un problème	Lecture			
GetIssueTextSummary [autorisation uniquement]	Accorde l'autorisation d'obtenir un résumé textuel généré d'un problème	Lecture			
GetQuestionnaire [autorisation uniquement]	Accorde l'autorisation de recevoir un questionnaire de commentaires	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SaveFeedback [autorisation uniquement]	Accorde l'autorisation d'enregistrer les commentaires du questionnaire	Écrire			

Types de ressources définis par AWS Support la console

AWS Support La console ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à la console AWS Support , spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Support console

La console de support ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les AWS Support plans

AWS Support Plans (préfixe de service :`supportplans`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les AWS Support plans
- Types de ressources définis par les AWS Support plans
- Clés de condition pour les AWS Support plans

Actions définies par les AWS Support plans

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSupportPlanSchedule [autorisation uniquement]	Accorde l'autorisation de créer des plannings de plan de support pour cela Compte AWS	Écrire			
GetSupportPlan [autorisation uniquement]	Accorde l'autorisation d'afficher les détails du plan de support actuel pour cela Compte AWS	Lecture			
GetSupportPlanUpdateStatus [autorisation uniquement]	Accorde l'autorisation d'afficher des détails sur l'état d'une demande de mise à jour d'un plan de support	Lecture			
ListSupportPlanModifiers	Accorde l'autorisation de consulter une liste de tous les modificateurs du	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]	plan de support pour cela Compte AWS				
StartSupportPlanUpdate [autorisation uniquement]	Accorde l'autorisation de mettre à jour le plan de support pour cela Compte AWS	Écrire			

Types de ressources définis par les AWS Support plans

AWS Support Plans ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Support Plans, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour les AWS Support plans

Support Plans ne dispose d'aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des instructions de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour le AWS développement durable

AWS Sustainability (préfixe de service :`sustainability`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.

- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS développement durable
- Types de ressources définis par AWS Sustainability
- Clés de condition pour le AWS développement durable

Actions définies par le AWS développement durable

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetCarbonFootprintSummary	Accorde l'autorisation de consulter l'outil de l'empreinte carbone.	Lecture			
GetEstimatedCarbonEmissions	Permet de consulter les valeurs d'émissions de carbone estimées en fonction du regroupement de clients et des paramètres de filtrage	Lecture			
GetEstimatedCarbonEmissions	Permet de visualiser les valeurs dimensionnelles possibles disponibles pour les	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Dimension Values	valeurs d'émission de carbone estimées				

Types de ressources définis par AWS Sustainability

AWS La durabilité ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à la durabilité AWS , spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour le AWS développement durable

La durabilité ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Systems Manager for SAP

AWS Systems Manager for SAP (préfixe de service :`ssm-sap`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Systems Manager pour SAP

- Types de ressources définis par AWS Systems Manager pour SAP
- Clés de condition pour AWS Systems Manager for SAP

Actions définies par AWS Systems Manager pour SAP

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BackupDatabase	Accorde l'autorisation d'exécuter une opération de sauvegarde sur une base de données spécifiée	Écrire			
DeleteResourcePermission	Accorde l'autorisation de supprimer le SSM pour les autorisations de ressources de niveau SAP associées à une ressource de base de données SSM pour SAP	Gestion des autorisations			
DeregisterApplication	Accorde l'autorisation de désinscrire une application SAP avec SSM pour SAP	Écrire	application		
GetApplication	Accorde l'autorisation d'accéder aux informations relatives à une application enregistrée auprès de SSM	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	pour SAP en fournissant l'ID ou l'ARN de l'application				
GetComponent	Accorde l'autorisation d'accéder aux informations relatives à un composant enregistré auprès de SSM pour SAP en fournissant l'ID de l'application et l'ID du composant	Lecture	component		
GetConfigurationCheckOperation	Accorde l'autorisation d'obtenir les détails d'une opération de vérification de configuration en spécifiant l'ID de l'opération	Lecture			
GetDatabase	Accorde l'autorisation d'accéder aux informations relatives à une base de données enregistrée auprès de SSM pour SAP en fournissant l'ID de l'application, l'ID du composant et l'ID de base de données	Lecture			
GetOperation	Accorde l'autorisation d'accéder aux informations relatives à une opération en fournissant son ID d'opération	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourcePermission	Accorde l'autorisation d'obtenir les autorisations de ressources de niveau SSM pour SAP associées à une ressource de base de données SSM pour SAP	Gestion des autorisations			
ListApplications	Autorise le client à récupérer la liste de toutes les applications enregistrées auprès de SSM pour SAP Compte AWS	List			
ListComponents	Accorde l'autorisation de récupérer une liste de toutes les composantes du compte du client ou d'une application spécifique	List	application		
ListConfigurationCheckDefinitions	Autorise à répertorier tous les types de contrôles de configuration pris en charge par AWS Systems Manager for SAP	List			
ListConfigurationCheckOperations	Accorde l'autorisation de répertorier les opérations de vérification de configuration passées	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDatabases	Accorde l'autorisation de récupérer une liste de toutes les bases de données du compte du client ou d'une application spécifique	List			
ListOperationEvents	Accorde l'autorisation de récupérer une liste de tous les événements d'une opération spécifiée	List			
ListOperations	Accorde l'autorisation de récupérer une liste de toutes les opérations sur le compte du client, des filtres supplémentaires peuvent être appliqués	List			
ListSubCheckResults	Accorde l'autorisation de répertorier les résultats des sous-vérifications d'une opération de vérification de configuration spécifiée	List			
ListSubCheckRuleResults	Accorde l'autorisation de répertorier les règles d'une sous-vérification spécifiée appartenant à une opération de vérification de configuration	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises sur l'ARN d'une ressource spécifiée	Lecture			
PutResourcePermission	Accorde l'autorisation d'ajouter les autorisations de ressources de niveau SSM pour SAP associées à une ressource de base de données SSM pour SAP	Gestion des autorisations			
RegisterApplication	Accorde l'autorisation d'inscrire une application SAP avec SSM pour SAP	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
RestoreDatabase	Accorde l'autorisation de restaurer une base de données à partir d'une autre base de données	Écrire			
StartApplication	Accorde l'autorisation de démarrer une application SSM enregistrée pour SAP	Écrire	application		
StartApplicationRefresh	Octroie l'autorisation de lancer une découverte à la demande d'une application SSM pour SAP enregistrée.	Écrire	application		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartConfigurationChecks	Accorde l'autorisation d'initier des opérations de vérification de configuration sur une application spécifiée	Écrire			
StopApplication	Autorise l'arrêt d'une application SSM enregistrée pour SAP	Écrire	application		
TagResource	Accorde l'autorisation de baliser l'ARN d'une ressource spécifiée	Identification	application		
			component		
			database		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises de l'ARN d'une ressource spécifiée	Identification	application		
			component		
			database		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateApplicationSettings	Accorde l'autorisation de mettre à jour les paramètres d'une application SSM pour SAP inscrite	Écrire	application		
UpdateHANABackupSettings	Accorde l'autorisation de mettre à jour les paramètres de sauvegarde HANA d'une base de données spécifiée	Écrire			

Types de ressources définis par AWS Systems Manager pour SAP

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
application	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/COMPONENT/${ComponentId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
database	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/DB/${DatabaseId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Systems Manager for SAP

AWS Systems Manager for SAP définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Systems Manager GUI Connect

AWS Systems Manager GUI Connect (préfixe de service :`ssm-guiconnect`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Systems Manager GUI Connect
- Types de ressources définis par AWS Systems Manager GUI Connect
- Clés de condition pour AWS Systems Manager GUI Connect

Actions définies par AWS Systems Manager GUI Connect

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelConnection [autorisation uniquement]	Accorde l'autorisation de mettre fin à une connexion GUI Connect	Écrire			
DeleteConnectionRecordingPreferences	Accorde l'autorisation de supprimer les préférences d'enregistrement de connexion GUI Connect	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetConnection [autorisation uniquement]	Accorde l'autorisation d'obtenir les métadonnées pour une connexion GUI Connect	Lecture			
GetConnectionRecordingPreferences	Accorde l'autorisation d'obtenir les préférences d'enregistrement de la connexion GUI Connect	Lecture			
ListConnections [autorisation uniquement]	Accorde l'autorisation de répertorier les métadonnées pour les connexions GUI Connect	List			
StartConnection [autorisation uniquement]	Accorde l'autorisation de démarrer une connexion GUI Connect	Écrire			
UpdateConnectionRecordingPreferences	Accorde l'autorisation de mettre à jour les préférences d'enregistrement de la connexion GUI Connect	Écrire			

Types de ressources définis par AWS Systems Manager GUI Connect

AWS Systems Manager GUI Connect ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Systems Manager GUI Connect, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Systems Manager GUI Connect

GUI Connect ne comporte pas de clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager (préfixe de service :`ssm-incidents`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Systems Manager Incident Manager
- Types de ressources définis par AWS Systems Manager Incident Manager
- Clés de condition pour AWS Systems Manager Incident Manager

Actions définies par AWS Systems Manager Incident Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetIncidentFindings	Accorde l'autorisation de récupérer des informations sur des résultats spécifiques pour un dossier d'incident	Lecture	incident-record*		
			response-plan*		
CreateReplicationSet	Accorde l'autorisation de créer un ensemble de réplications.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole ssm-incidents:TagResource
CreateResponsePlan	Accorde l'autorisation de créer un plan de réponse.	Écriture		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole ssm-incidents:TagResource
CreateTimelineEvent	Accorde l'autorisation de créer un événement chronologique pour un dossier d'incident.	Écriture	incident-record*		
			response-plan*		
DeleteIncidentRecord	Accorde l'autorisation de supprimer un dossier d'incident.	Écriture	incident-record*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteReplicationSet	Accorde l'autorisation de supprimer un ensemble de réplications.	Écriture	replication-set*		
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource d'un plan de réponse.	Gestion des autorisations	response-plan*		
DeleteResponsePlan	Accorde l'autorisation de supprimer un plan de réponse.	Écriture	response-plan*		
DeleteTimelineEvent	Accorde l'autorisation de supprimer un événement chronologique.	Écriture	incident-record*		
GetIncidentRecord	Accorde l'autorisation d'afficher le contenu d'un dossier d'incident.	Lecture	incident-record*		
			response-plan*		
GetReplicationSet	Accorde l'autorisation d'afficher l'ensemble de réplications.	Lecture	replication-set*		
GetResourcePolicies	Accorde l'autorisation d'afficher des stratégies de ressource d'un plan de réponse.	Lecture	response-plan*		
GetResponsePlan	Accorde l'autorisation d'afficher le contenu d'un plan de réponse spécifié.	Lecture	response-plan*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTimelineEvent	Accorde l'autorisation d'afficher un événement chronologique.	Lecture	incident-record*		
			response-plan*		
ListIncidentFindings	Accorde l'autorisation de répertorier les résultats d'un dossier d'incident	List	incident-record*		
			response-plan*		
ListIncidentRecords	Accorde l'autorisation de répertorier les contenus de tous les dossiers d'incidents	List			
ListRelatedItems	Accorde l'autorisation de répertorier des éléments liés à un dossier d'incident	List	incident-record*		
			response-plan*		
ListReplicationSets	Accorde l'autorisation de répertorier tous les ensembles de réplication.	Liste			
ListResponsePlans	Accorde l'autorisation de répertorier tous les plans de réponse.	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation d'afficher une liste de identifications de ressource pour une ressource spécifiée	Lecture	incident-record		
			replication-set		
			response-plan		
ListTimelineEvents	Accorde l'autorisation de répertorier tous les événements chronologiques d'un dossier d'incident.	Liste	incident-record*		
			response-plan*		
PutResourcePolicy	Accorde l'autorisation de placer une politique de ressource dans un plan de réponse.	Gestion des autorisations	response-plan*		
StartIncident	Accorde l'autorisation d'aborder un nouvel incident à l'aide d'un plan de réponse	Écriture	response-plan*		
TagResource	Accorde l'autorisation d'ajouter des balises à un plan de réponse.	Balisage	incident-record		
			replication-set		
			response-plan		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des balises d'un plan de réponse.	Balisage	incident-record		
			replication-set		
			response-plan		
				aws:TagKeys	
UpdateDeletionProtection	Accorde l'autorisation de mettre à jour la protection contre la suppression des ensembles de réplication.	Écriture	replication-set*		
UpdateIncidentRecord	Accorde l'autorisation de mettre à jour le contenu d'un dossier d'incident.	Écriture	incident-record*		
			response-plan*		
UpdateRelatedItems	Accorde l'autorisation de mettre à jour des éléments liés d'un dossier d'incident.	Écriture	incident-record*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			response-plan*		
UpdateReplicationSet	Accorde l'autorisation de mettre à jour un ensemble de réplication.	Écriture	replication-set*		
UpdateResponsePlan	Accorde l'autorisation de mettre à jour le contenu d'un plan de réponse.	Écriture	response-plan*		iam:PassRole ssm-incidents:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTimelineEvent	Accorde l'autorisation de mettre à jour un événement chronologique.	Écrire	incident-record*		
			response-plan*		

Types de ressources définis par AWS Systems Manager Incident Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
response-plan	`arn:${Partition}:ssm-incidents::${Account}:response-plan/${ResponsePlan}`	aws:ResourceTag/${TagKey}
incident-record	`arn:${Partition}:ssm-incidents::${Account}:incident-record/${ResponsePlan}/${IncidentRecord}`	aws:ResourceTag/${TagKey}
replication-set	`arn:${Partition}:ssm-incidents::${Account}:replication-set/${ReplicationSet}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les contacts de AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager Contacts (préfixe de service :`ssm-contacts`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les contacts AWS de Systems Manager Incident Manager
- Types de ressources définis par les contacts AWS de Systems Manager Incident Manager
- Clés de condition pour les contacts de AWS Systems Manager Incident Manager

Actions définies par les contacts AWS de Systems Manager Incident Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptPage	Accorde l'autorisation d'accepter une page.	Écriture	page*		
ActivateContactChannel	Accorde l'autorisation d'activer le canal de contact d'un contact.	Écriture	contactchannel*		
AssociateContact [autorisation uniquement]	Accorde l'autorisation d'utiliser un contact dans un plan d'escalade.	Gestion des autorisations	contact*		
CreateContact	Accorde l'autorisation de créer un contact	Écriture	contact*		ssm-contacts:AssociateContact
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContactChannel	Accorde l'autorisation de créer un canal de contact pour un contact.	Écrire	contact*		
CreateRotation	Accorde l'autorisation de créer une rotation dans un programme de veille	Écrire	rotation*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey}	
CreateRotationOverride	Accorde l'autorisation de créer un chevauchement de rotation dans un programme de veille	Écrire	rotation*		
DeactivateContactChannel	Accorde l'autorisation de désactiver le canal de contact d'un contact.	Écriture	contactchannel*		
DeleteContact	Accorde l'autorisation de supprimer un contact.	Écriture	contact*		
DeleteContactChannel	Accorde l'autorisation de supprimer le canal de contact d'un contact.	Écrire	contactchannel*		
DeleteRotation	Accorde l'autorisation de supprimer une rotation	Écrire	rotation*		
DeleteRotationOverride	Accorde l'autorisation de supprimer le chevauchement d'une rotation	Écrire	rotation*		
DescribeEngagement	Accorde l'autorisation de décrire un engagement.	Lecture	engagement*		
DescribePage	Accorde l'autorisation de décrire une page.	Lecture	page*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetContact	Accorde l'autorisation d'obtenir un contact.	Lecture	contact*		
GetContactChannel	Accorde l'autorisation d'obtenir le canal de contact d'un contact.	Lecture	contactchannel*		
GetContactPolicy	Accorde l'autorisation d'obtenir la stratégie de ressource d'un contact	Lecture	contact*		
GetRotation	Accorde l'autorisation de récupérer les informations sur une rotation dans un programme de veille	Lecture	rotation*		
GetRotationOverride	Accorde l'autorisation de récupérer les informations sur le chevauchement d'une rotation dans un programme de veille	Lecture	rotation*		
ListContactChannels	Accorde l'autorisation de répertorier tous les canaux de contact d'un contact.	Liste	contact*		
ListContacts	Accorde l'autorisation de répertorier tous les contacts.	Liste			
ListEngagements	Accorde l'autorisation de répertorier tous les engagements	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPageReceipts	Accorde l'autorisation de répertorier tous les reçus d'une page.	List	page*		
ListPageResolutions	Octroie l'autorisation de répertorier le chemin de résolution d'un engagement.	List	page*		
ListPagesByContact	Accorde l'autorisation de répertorier toutes les pages envoyées à un contact.	Liste	contact*		
ListPagesByEngagement	Accorde l'autorisation de répertorier toutes les pages créées dans un engagement.	List	engagement*		
ListPreviewRotationShifts	Accorde l'autorisation de récupérer une liste de changements en fonction des paramètres de configuration de la rotation	List			
ListRotationOverrides	Accorde l'autorisation de récupérer une liste des chevauchements actuellement spécifiés pour une rotation dans un programme de veille	List	rotation*		
ListRotationShifts	Accorde l'autorisation de créer des changements de rotation dans un programme de veille	List	rotation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRotations	Accorde l'autorisation de récupérer une liste des rotations dans un programme de veille	List			
ListTagsForResource	Accorde l'autorisation d'afficher une liste de identifications de ressource pour une ressource spécifiée	Lecture	contact rotation		
PutContactPolicy	Accorde l'autorisation d'ajouter une politique de ressource à un contact.	Écriture	contact*		
SendActivationCode	Accorde l'autorisation d'envoyer le code d'activation du canal de contact d'un contact.	Écriture	contactchannel*		
StartEngagement	Accorde l'autorisation de démarrer un engagement.	Écriture	contact*		
StopEngagement	Accorde l'autorisation d'arrêter un engagement.	Écrire	engagement*		
TagResource	Accorde l'autorisation d'ajouter des balises à la ressource spécifiée	Identification	contact rotation		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les balises de la ressource spécifiée	Identification	contact rotation		
				aws:TagKeys	
UpdateContact	Accorde l'autorisation de mettre à jour un contact.	Écriture	contact*		ssm-contacts:AssociateContact
UpdateContactChannel	Accorde l'autorisation de mettre le canal de contact d'un contact.	Écrire	contactchannel*		
UpdateRotation	Accorde l'autorisation de mettre à jour les informations spécifiées pour une rotation dans un programme de veille	Écrire	rotation*		

Types de ressources définis par les contacts AWS de Systems Manager Incident Manager

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
contact	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contact/${ContactAlias}`	aws:ResourceTag/${TagKey}
contactchannel	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contactchannel/${ContactAlias}/${ContactChannelId}`	
engagement	`arn:${Partition}:ssm-contacts:${Region}:${Account}:engagement/${ContactAlias}/${EngagementId}`	
page	`arn:${Partition}:ssm-contacts:${Region}:${Account}:page/${ContactAlias}/${PageId}`	
rotation	`arn:${Partition}:ssm-contacts:${Region}:${Account}:rotation/${RotationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les contacts de AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager Contacts définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour

affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour la configuration rapide de AWS Systems Manager

AWS La configuration rapide de Systems Manager (préfixe de service :`ssm-quicksetup`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Systems Manager Quick Setup
- Types de ressources définis par AWS Systems Manager Quick Setup
- Clés de condition pour la configuration rapide de AWS Systems Manager

Actions définies par AWS Systems Manager Quick Setup

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateConfigurationManager	Accorde l'autorisation de créer une ressource du gestionnaire de configuration Quick Setup	Écrire	configuration-manager*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteConfigurationManager	Accorde l'autorisation de supprimer un gestionnaire de configuration	Écrire	configuration-manager*		
GetConfiguration	Accorde l'autorisation d'obtenir la configuration de configuration rapide	Lecture	configuration-manager		
GetConfigurationManager	Accorde l'autorisation d'obtenir un gestionnaire de configuration	Lecture	configuration-manager*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetServiceSettings	Accorde l'autorisation de configurer les paramètres pour la configuration rapide dans le formulaire de demande Compte AWS et Région AWS	Lecture			
ListConfigurationManagers	Accorde l'autorisation de répertorier les gestionnaires de configuration Quick Setup	List			
ListConfigurations	Accorde l'autorisation de répertorier les configurations de configuration rapide	List	configuration-manager		
ListQuickSetupTypes	Accorde l'autorisation de répertorier les types de configuration rapide disponibles	Lecture			
ListTagsForResource	Accorde l'autorisation de répertorier les balises attribuées à la ressource	Lecture	configuration-manager*		
TagResource	Accorde l'autorisation d'attribuer des paires clé-valeur de métadonnées aux ressources AWS	Identification	configuration-manager*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer les balises de la ressource spécifiée	Identification	configuration-manager*		
				aws:TagKeys	
UpdateConfigurationDefinition	Autorise la mise à jour d'une définition de configuration Quick Setup	Écrire	configuration-manager*		
UpdateConfigurationManager	Autorise la mise à jour d'un gestionnaire de configuration Quick Setup	Écrire	configuration-manager*		
UpdateServiceSettings	Accorde l'autorisation de mettre à jour les paramètres configurés pour la configuration rapide	Écrire			

Types de ressources définis par AWS Systems Manager Quick Setup

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
configuration-manager	`arn:${Partition}:ssm-quicksetup:${Region}:${Account}:configuration-manager/${ConfigurationManagerId}`	aws:ResourceTag/${TagKey}

Clés de condition pour la configuration rapide de AWS Systems Manager

AWS La configuration rapide de Systems Manager définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Tag Editor

L'éditeur de balises (préfixe de service :`resource-explorer`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Tag Editor
- Types de ressources définis par Tag Editor
- Clés de condition pour Tag Editor

Actions définies par Tag Editor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceTypes [autorisation uniquement]	Accorde l'autorisation de récupérer les types de ressources actuellement pris en charge par Tag Editor	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResources [autorisation uniquement]	Accorde l'autorisation de récupérer les identifiants des ressources dans le Compte AWS	List			
ListTags [autorisation uniquement]	Accorde l'autorisation de récupérer les balises attachées aux identificateurs de ressources spécifiés	Lecture			tag:GetResources

Types de ressources définis par Tag Editor

L'éditeur de balises ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Tag Editor, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Tag Editor

Tag Editor ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les paramètres AWS fiscaux

AWS Les paramètres fiscaux (préfixe de service :`tax`) fournissent les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les paramètres AWS fiscaux
- Types de ressources définis par les paramètres AWS fiscaux
- Clés de condition pour les paramètres AWS fiscaux

Actions définies par les paramètres AWS fiscaux

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchDeleteTaxRegistration	Autorise la suppression par lots des données d'enregistrement fiscal	Écrire			
BatchPutTaxRegistration	Accorde l'autorisation de mettre à jour par lot les données des immatriculations fiscales	Écrire			
CancelDocument	Autorise l'annulation de documents tels que les bordereaux de retenue	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDocument	Autorise le téléchargement de nouveaux documents tels que des bordereaux de retenue	Écrire			
DeleteSupplementalTaxRegistration	Autorise la suppression des données d'enregistrement fiscal supplémentaires	Écrire			
DeleteTaxRegistration	Accorde l'autorisation d'effacer les données des immatriculations fiscales	Écrire			
GetDocument	Permet de récupérer des documents tels que des bordereaux de retenue	Lecture			
GetDocumentUploadUrl	Accorde l'autorisation de récupérer une URL générée pour télécharger des documents	Lecture			
GetExemptions	Accorde l'autorisation d'afficher les données des exonérations fiscales	Lecture			
GetTaxInfoReportingDocument [autorisation uniquement]	Donne l'autorisation d'établir des view/download documents /formulaires fiscaux	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTaxInheritance	Accorde l'autorisation d'afficher le statut d'héritage fiscal	Lecture			
GetTaxInterview [autorisation uniquement]	Accorde l'autorisation de récupérer les données d'un questionnaire fiscal	Lecture			
GetTaxRegistration	Accorde l'autorisation d'afficher les données des immatriculations fiscales	Lecture			
GetTaxRegistrationDocument	Accorde l'autorisation de télécharger les immatriculations fiscales	Lecture			
ListDocuments	Autorise l'accès à des documents tels que des bordereaux de retenue	Lecture			
ListSupplementalTaxRegistrations	Donne l'autorisation de consulter les enregistrements fiscaux supplémentaires	Lecture			
ListTaxRegistrations	Accorde l'autorisation d'afficher les immatriculations fiscales	Lecture			
ListWithholdingEligibleInvoices	Permet de consulter les factures de retenue éligibles	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutSupplementalTaxRegistration	Autorise la mise à jour des données d'enregistrement fiscal supplémentaires	Écrire			
PutTaxInheritance	Accorde l'autorisation d'établir le statut d'héritage fiscal	Écrire			
PutTaxInterview [autorisation uniquement]	Accorde l'autorisation de mettre à jour les données d'un questionnaire fiscal	Écrire			
PutTaxRegistration	Accorde l'autorisation de mettre à jour les données des immatriculations fiscales	Écrire			
UpdateExemptions	Accorde l'autorisation de mettre à jour les données des exonérations fiscales	Écrire			

Types de ressources définis par les paramètres AWS fiscaux

AWS Les paramètres fiscaux ne permettent pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Paramètres de taxes, précisez `"Resource": "*"` dans votre politique.

Clés de condition pour les paramètres AWS fiscaux

Paramètres de taxes ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour AWS Telco Network Builder

AWS Telco Network Builder (préfixe de service :tnb) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Telco Network Builder
- Types de ressources définis par AWS Telco Network Builder
- Clés de condition pour AWS Telco Network Builder

Actions définies par AWS Telco Network Builder

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à

utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelSolNetworkOperation	Accorde l'autorisation d'annuler une opération de réseau	Écrire	network-operation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSolFunctionPackage	Accorde l'autorisation de créer un package de fonction	Écrire	function-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkInstance	Accorde l'autorisation de créer une instance de réseau	Écrire	network-instance*		
			network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkPackage	Accorde l'autorisation de créer un package réseau	Écrire	network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSolFunctionPackage	Accorde l'autorisation de supprimer un package de fonction	Écrire	function-package*		
DeleteSolNetworkInstance	Accorde l'autorisation de supprimer une instance de réseau	Écrire	network-instance*		
DeleteSolNetworkPackage	Accorde l'autorisation de supprimer un package de réseau	Écrire	network-package*		
GetSolFunctionInstance	Accorde l'autorisation d'obtenir une instance de fonction	Lecture	function-instance*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackage	Accorde l'autorisation d'obtenir un package de fonctions	Lecture	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageContent	Accorde l'autorisation d'obtenir le contenu d'un package de fonctions	Lecture	function-package*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSolFunctionPackageDescriptor	Accorde l'autorisation d'obtenir un descripteur de package	Lecture	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkInstance	Accorde l'autorisation d'obtenir une instance de réseau	Lecture	network-instance*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkOperation	Accorde l'autorisation d'obtenir une opération de réseau	Lecture	network-operation*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackage	Accorde l'autorisation d'obtenir un package de réseau	Lecture	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageContent	Accorde l'autorisation d'obtenir le contenu d'un service	Lecture	network-package*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageDescriptor	Accorde l'autorisation d'obtenir un descripteur de package	Lecture	network-package*		
				aws:ResourceTag/${TagKey}	
InstantiateSolNetworkInstance	Accorde l'autorisation d'arrêter une instance	Écrire	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListSolFunctionInstances	Accorde l'autorisation de répertorier les instances de fonction	List	function-instance*		
				aws:ResourceTag/${TagKey}	
ListSolFunctionPackages	Accorde l'autorisation de répertorier des packages de fonctions	List	function-package*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ListSolNetworkInstances	Accorde l'autorisation de répertorier les instances de réseaux	List	network-instance*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkOperations	Accorde l'autorisation de répertorier les opérations de réseaux	List	network-operation*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkPackages	Accorde l'autorisation de répertorier les packages de réseaux	List	network-package*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Accorde l'autorisation de renvoyer une liste d'étiquettes pour une ressource	List			
PutSolFunctionPackageContent	Accorde l'autorisation de charger le contenu du service	Écrire	function-package*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutSolNetworkPackageContent	Accorde l'autorisation de charger le contenu du service	Écrire	network-package*		
TagResource	Accorde l'autorisation d'ajouter des balises à la ressource spécifiée	Identification	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateSolNetworkInstance	Accorde l'autorisation de terminer une instance de réseau	Écrire	network-instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les balises de la ressource spécifiée	Identification	function-instance		
			function-package		
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys	
UpdateSolFunctionPackage	Accorde l'autorisation de mettre à jour un package de fonction	Écrire	function-package*		
UpdateSolNetworkInstance	Accorde l'autorisation de mettre à jour une instance de réseau	Écrire	function-instance*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSolNetworkPackage	Accorde l'autorisation de mettre à jour un package de réseau	Écrire	network-package*		
ValidateSolFunctionPackageContent	Accorde l'autorisation de valider le contenu du package de fonction	Écrire	function-package*		
ValidateSolNetworkPackageContent	Accorde l'autorisation de valider le contenu du package de réseau	Écrire	network-package*		

Types de ressources définis par AWS Telco Network Builder

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
function-package	arn:${Partition}:tnb:${Region}:${Account}:function-package/${FunctionPackageId}	aws:ResourceTag/${TagKey}
network-package	arn:${Partition}:tnb:${Region}:${Account}:network-package/${NetworkPackageId}	aws:ResourceTag/${TagKey}
network-instance	arn:${Partition}:tnb:${Region}:${Account}:network-instance/${NetworkInstanceId}	aws:ResourceTag/${TagKey}
function-instance	arn:${Partition}:tnb:${Region}:${Account}:function-instance/${FunctionInstanceId}	aws:ResourceTag/${TagKey}
network-operation	arn:${Partition}:tnb:${Region}:${Account}:network-operation/${NetworkOperationId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Telco Network Builder

AWS Telco Network Builder définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en vérifiant la présence de paires clé-valeur de balise dans la demande	String

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en vérifiant les paires clé-valeur de balise attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés de balise dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Textract

Amazon Textract (préfixe de service : `textract`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Textract
- Types de ressources définis par Amazon Textract
- Clés de condition pour Amazon Textract

Actions définies par Amazon Textract

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AnalyzeDocument	Accorde l'autorisation de détecter les instances d'entités de document réelles au sein d'une image fournie comme entrée	Lecture			s3:GetObject
AnalyzeExpense	Accorde l'autorisation de détecter les instances d'entités de document réelles au sein d'une image fournie comme entrée	Lecture			s3:GetObject
AnalyzeID	Accorde l'autorisation de détecter des informations pertinentes à partir de documents d'identité fournis comme entrée	Lecture			s3:GetObject
CreateAdapter	Accorde l'autorisation de créer un adaptateur Amazon Textract.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdapterVersion	Accorde l'autorisation de créer une version de l'adaptateur Amazon Textract.	Écrire	adapter*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DeleteAdapter	Accorde l'autorisation de supprimer un adaptateur Amazon Textract.	Écrire	adapter*		
DeleteAdapterVersion	Accorde l'autorisation de supprimer une version de l'adaptateur Amazon Textract.	Écrire	adapterversion*		
DetectDocumentText	Accorde l'autorisation de détecter du texte dans des images de document	Lecture			s3:GetObject
GetAdapter	Accorde l'autorisation d'obtenir un adaptateur Amazon Textract.	Lecture	adapter*		
GetAdapterVersion	Accorde l'autorisation d'obtenir une version de l'adaptateur Amazon Textract.	Lecture	adapterversion*		
GetDocumentAnalysis	Accorde l'autorisation de renvoyer des informations sur une tâche d'analyse de documents	Lecture			
GetDocumentTextDetection	Accorde l'autorisation de renvoyer des informations sur une tâche de détection de texte de document	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetExpenseAnalysis	Accorde l'autorisation de renvoyer des informations sur une tâche d'analyse de dépenses	Lecture			
GetLendingAnalysis	Accorde l'autorisation de récupérer des informations au niveau de la page concernant une tâche d'analyse de prêt	Lecture			
GetLendingAnalysisSummary	Accorde l'autorisation de récupérer des informations résumées concernant une tâche d'analyse de prêt	Lecture			
ListAdapterVersions	Accorde l'autorisation de répertorier les versions des adaptateurs Amazon Textract.	Lecture			
ListAdapters	Accorde l'autorisation de répertorier les adaptateurs Amazon Textract.	Lecture			
ListTagsForResource	Accorde l'autorisation de renvoyer une liste de balises associées à une ressource	Lecture	adapter		
			adapterversion		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartDocumentAnalysis	Accorde l'autorisation de démarrer une tâche asynchrone pour détecter les instances d'entités de document réelles au sein d'une image ou d'un fichier pdf fourni en entrée	Écrire			s3:GetObject
StartDocumentTextDetection	Accorde l'autorisation de démarrer une tâche asynchrone pour détecter du texte dans les images de document ou les fichiers pdf	Écrire			s3:GetObject
StartExpenseAnalysis	Accorde l'autorisation de démarrer une tâche asynchrone pour détecter les instances de factures ou reçus au sein d'une image ou d'un fichier pdf fourni comme entrée	Écrire			s3:GetObject
StartLendingAnalysis	Accorde l'autorisation de démarrer une tâche asynchrone pour la détection d'entités dans un document de prêt, en prenant une image ou un PDF fournis comme entrée	Écrire			s3:GetObject
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une ressource	Balisage	adapter		
			adapterversion		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Identification	adapter		
			adapterversion		
				aws:TagKeys	
UpdateAdapter	Accorde l'autorisation de mettre à jour l'adaptateur Amazon Textract.	Écrire	adapter*		

Types de ressources définis par Amazon Textract

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
adapter	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}`	aws:ResourceTag/${TagKey}
adapterversion	`arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}/versions/${AdapterVersion}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Textract

Amazon Textract définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des balises transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des balises associées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés de balise transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Timestream

Amazon Timestream (préfixe de service : `timestream`) fournit les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Timestream
- Types de ressources définis par Amazon Timestream
- Clés de condition pour Amazon Timestream

Actions définies par Amazon Timestream

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CancelQuery	Accorde l'autorisation d'annuler des requêtes dans votre compte	Écrire			timestream:DescribeEndpoints
CreateBatchLoadTask	Octroie l'autorisation de créer une tâche de chargement par lots dans votre compte	Écrire	table*		timestream:DescribeEndpoints

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					timestream:WriteRecords
CreateDatabase	Accorde l'autorisation de créer une base de données dans votre compte	Écrire	database*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledQuery	Accorde l'autorisation de créer une requête planifiée dans votre compte	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole timestream:DescribeEndpoints
CreateTable	Accorde l'autorisation de créer une table dans votre compte.	Écrire	table*		timestream:DescribeEndpoints

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatabase	Accorde l'autorisation de supprimer une base de données de votre compte	Écrire	database*		timestream:DescribeEndpoints
DeleteScheduledQuery	Accorde l'autorisation de supprimer une requête planifiée de votre compte	Écrire	scheduled-query*		timestream:DescribeEndpoints
DeleteTable	Accorde l'autorisation de supprimer une table de votre compte	Écrire	table*		timestream:DescribeEndpoints
DescribeAccountSettings	Accorde l'autorisation de décrire les paramètres de votre compte	Lecture			timestream:DescribeEndpoints
DescribeBatchLoadTask	Octroie l'autorisation de décrire une tâche de chargement par lots dans votre compte	Lecture			timestream:DescribeEndpoints

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeDatabase	Accorde l'autorisation de décrire une base de données dans votre compte	Lecture	database*		timestream:DescribeEndpoints
DescribeEndpoints	Accorde l'autorisation de décrire les points de terminaison Timestream	List			
DescribeScheduledQuery	Accorde l'autorisation de décrire une requête planifiée dans votre compte	Lecture	scheduled-query*		timestream:DescribeEndpoints
DescribeTable	Accorde l'autorisation de décrire une table dans votre compte	Lecture	table*		timestream:DescribeEndpoints
ExecuteScheduledQuery	Accorde l'autorisation d'exécuter une requête planifiée dans votre compte	Écrire	scheduled-query*		timestream:DescribeEndpoints
GetAwsBackupStatus	Accorde l'autorisation d'obtenir le statut d'une sauvegarde de table Timestream	Lecture			timestream:DescribeEndpoints

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAwsRestoreStatus	Accorde l'autorisation d'obtenir le statut d'une restauration de table Timestream	Lecture			timestream:DescribeEndpoints
ListBatchLoadTasks	Octroie l'autorisation de répertorier les tâches de chargement par lots dans votre compte	List			timestream:DescribeEndpoints
ListDatabases	Accorde l'autorisation de répertorier les bases de données de votre compte	List			timestream:DescribeEndpoints
ListMeasures	Accorde l'autorisation de répertorier les mesures d'une table de votre compte	List	table*		timestream:DescribeEndpoints
ListScheduledQueries	Accorde l'autorisation de répertorier les requêtes planifiées de votre compte	List			timestream:DescribeEndpoints
ListTables	Accorde l'autorisation de répertorier les tables de votre compte	List	database*		timestream:DescribeEndpoints

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource de votre compte	Lecture	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
PrepareQuery	Accorde l'autorisation d'émettre des requêtes de préparation	Lecture	table*		timestream:DescribeEndpoints timestream:Select
ResumeBatchLoadTask	Octroie l'autorisation de relancer une tâche de chargement par lots dans votre compte	Écrire			timestream:DescribeEndpoints timestream:WriteRecords
Select	Accorde l'autorisation d'émettre des requêtes « select from table »	Lecture	table*		timestream:DescribeEndpoints

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SelectValues	Accorde l'autorisation d'émettre des requêtes « select 1 »	Lecture			timestream:DescribeEndpoints
StartAwsBackupJob	Accorde l'autorisation de démarrer une tâche de sauvegarde pour une table Timestream	Écrire	table*		timestream:DescribeEndpoints
StartAwsRestoreJob	Accorde l'autorisation de démarrer une tâche de restauration pour sauvegarde d'une table Timestream	Écrire	table*		timestream:DescribeEndpoints
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource	Identification	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Unload	Accorde l'autorisation d'émettre des requêtes de déchargement	Écrire	table*		s3:AbortMultipartUpload s3:GetObject s3:PutObject timestream:DescribeEndpoints timestream:Select
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAccountSettings	Autorise la mise à jour des paramètres de votre compte	Écrire			timestream:DescribeEndpoints
UpdateDatabase	Accorde l'autorisation de mettre à jour une base de données dans votre compte	Écrire	database*		timestream:DescribeEndpoints
UpdateScheduledQuery	Accorde l'autorisation de mettre à jour une requête enregistrée dans votre compte	Écrire	scheduled-query*		timestream:DescribeEndpoints
UpdateTable	Accorde l'autorisation de mettre à jour une table dans votre compte	Écrire	table*		timestream:DescribeEndpoints
WriteRecords	Accorde l'autorisation d'ingérer des données dans une table de votre compte	Écrire	table*		timestream:DescribeEndpoints

Types de ressources définis par Amazon Timestream

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
database	`arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}/table/${TableName}`	aws:ResourceTag/${TagKey}
scheduled-query	`arn:${Partition}:timestream:${Region}:${Account}:scheduled-query/${ScheduledQueryName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Timestream

Amazon Timestream définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identif ication dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Timestream InfluxDB

Amazon Timestream InfluxDB (préfixe de service `timestream-influxdb` :) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Timestream InfluxDB
- Types de ressources définis par Amazon Timestream InfluxDB
- Clés de condition pour Amazon Timestream InfluxDB

Actions définies par Amazon Timestream InfluxDB

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDbCluster	Accorde l'autorisation de créer un nouveau cluster Timestream InfluxDB	Écrire	db-parameter-group		timestream-influxdb:CreateDbInstance
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbInstance	Accorde l'autorisation de créer une nouvelle instance Timestream InfluxDB	Écrire	db-parameter-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbParameterGroup	Accorde l'autorisation de créer un nouveau groupe de paramètres Timestream InfluxDB	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDbCluster	Accorde l'autorisation de supprimer un cluster Timestream InfluxDB	Écrire	db-cluster*		timestream-influxdb:DeleteD

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					bInstance
DeleteDbInstance	Accorde l'autorisation de supprimer une instance Timestream InfluxDB	Écrire	db-instance*		
GetDbCluster	Accorde l'autorisation d'obtenir des informations sur un cluster Timestream InfluxDB	Lecture	db-cluster*		
GetDbInstance	Accorde l'autorisation d'obtenir des informations sur une instance Timestream InfluxDB	Lecture	db-instance*		
GetDbParameterGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de paramètres Timestream InfluxDB	Lecture	db-parameter-group*		
ListDbClusters	Accorde l'autorisation de répertorier les informations sur tous les clusters Timestream InfluxDB du compte	List			
ListDbInstances	Accorde l'autorisation de répertorier les informations sur toutes les instances Timestream InfluxDB du compte	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDbInstancesForCluster	Accorde l'autorisation de répertorier les informations sur toutes les instances Timestream InfluxDB appartenant à un cluster	Lecture	db-cluster*		
ListDbParameterGroups	Autorise à répertorier les informations sur tous les groupes de paramètres Timestream InfluxDB	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour une ressource Timestream InfluxDB	Lecture	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey}	
RebootDbCluster	Autorise le redémarrage d'un cluster Timestream InfluxDB	Écrire	db-cluster*		timestream-influxdb:RebootDbInstance
			db-instance		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RebootDbInstance	Autorise le redémarrage d'une instance Timestream InfluxDB	Écrire	db-instance*		
TagResource	Accorde l'autorisation de baliser une ressource Timestream InfluxDB	Identification	db-cluster		
			db-instance		
			db-parameter-group		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de détaguer une ressource Timestream InfluxDB	Identification	db-cluster		
			db-instance		
			db-parameter-group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDbCluster	Autorise la mise à jour d'un cluster Timestream InfluxDB	Écrire	db-cluster*		timestream-influxdb:UpdateDbInstance
			db-parameter-group		
UpdateDbInstance	Accorde l'autorisation de mettre à jour une instance Timestream InfluxDB	Écrire	db-instance*		
			db-parameter-group		

Types de ressources définis par Amazon Timestream InfluxDB

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
db-cluster	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-cluster/${DbClusterId}`	aws:ResourceTag/${TagKey}
db-instance	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-instance/${DbInstanceIdentifier}`	aws:ResourceTag/${TagKey}
db-parameter-group	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-parameter-group/${DbParameterGroupIdentifier}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Timestream InfluxDB

Amazon Timestream InfluxDB définit les clés de condition suivantes qui peuvent être utilisées dans `Condition` l'élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS Tiros

AWS Tiros (préfixe de service :`tiros`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Tiros
- Types de ressources définis par AWS Tiros
- Clés de condition pour AWS Tiros

Actions définies par AWS Tiros

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique

IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateQuery [autorisation uniquement]	Accorde l'autorisation de créer une requête d'accessibilité VPC	Écriture			
ExtendQuery [autorisation uniquement]	Accorde l'autorisation d'étendre la requête d'accessi	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	bilité d'un VPC pour inclure le compte du principal appelant				
GetQueryAnswer [autorisation uniquement]	Accorde l'autorisation d'obtenir des réponses de requête d'accessibilité VPC	Lecture			
GetQueryExplanation [autorisation uniquement]	Accorde l'autorisation pod'ur obtenir des explications de requête d'accessibilité VPC	Lecture			
GetQueryExtensionAccounts [autorisation uniquement]	Accorde l'autorisation de répertorier les comptes susceptibles d'être utiles dans une nouvelle requête	Lecture			

Types de ressources définis par AWS Tiros

AWS Tiros ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Tiros, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour AWS Tiros

Tiros ne dispose pas de clés de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des instructions de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Transcribe

Amazon Transcribe (préfixe de service : `transcribe`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Transcribe
- Types de ressources définis par Amazon Transcribe
- Clés de condition pour Amazon Transcribe

Actions définies par Amazon Transcribe

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateCallAnalyticsCategory	Accorde l'autorisation de créer une catégorie d'analyse Amazon Transcribe applique les conditions spécifiées par vos catégories d'analyse à vos tâches d'analyse d'appels	Écriture		aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateLanguageModel	Accorde l'autorisation de créer un modèle de langue personnalisé	Écriture		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateMedicalVocabulary	Accorde l'autorisation de créer un vocabulaire personnalisé que vous pouvez utiliser pour modifier la façon dont Amazon Transcribe Medical gère la transcription d'un fichier audio	Écriture		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateVocabulary	Accorde l'autorisation de créer un vocabulaire personnalisé que vous pouvez utiliser pour modifier la façon dont Amazon Transcribe gère la transcription d'un fichier audio	Écriture		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabularyFilter	Accorde l'autorisation de créer un nouveau filtre de vocabulaire que vous pouvez utiliser pour filtrer les mots provenant de la transcription d'un fichier audio généré par Amazon Transcribe	Écriture		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
DeleteCallAnalyticsCategory	Accorde l'autorisation de supprimer une catégorie d'analyse des appels à l'aide de son nom d'Amazon Transcribe	Écriture	callanalyticscategory*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteCallAnalyticsJob	Accorde l'autorisation de supprimer une tâche d'analyse des appels précédemment soumise ainsi que les résultats générés tels que la transcription, les modèles, et ainsi de suite	Écriture	callanalyticsjob*		
DeleteLanguageModel	Accorde l'autorisation de supprimer un modèle de langue personnalisé précédemment créé	Écrire	languagemodel*		
DeleteMedicalScribeJob	Octroie l'autorisation de supprimer une tâche de transcription médicale déjà soumise.	Écrire	medicalscribejob*		
DeleteMedicalTranscriptionJob	Accorde l'autorisation de supprimer une tâche de transcription médicale déjà soumise	Écriture	medicaltranscriptionjob*		
DeleteMedicalVocabulary	Accorde l'autorisation de supprimer un vocabulaire médical d'Amazon Transcribe	Écriture	medicalvocabulary*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteTranscriptionJob	Accorde l'autorisation de supprimer une tâche de transcription précédemment soumise ainsi que les résultats générés tels que la transcription, les modèles, et ainsi de suite	Écriture	transcriptionjob*		
DeleteVocabulary	Accorde l'autorisation de supprimer un vocabulaire d'Amazon Transcribe.	Écriture	vocabulary*		
DeleteVocabularyFilter	Accorde l'autorisation de supprimer un filtre de vocabulaire d'Amazon Transcribe	Écriture	vocabularyfilter*		
DescribeLanguageModel	Accorde l'autorisation de renvoyer des informations sur un modèle de langue personnalisé	Read	languagemodel*		
GetCallAnalyticsCategory	Accorde l'autorisation de récupérer des informations sur une catégorie d'analyse des appels	Read	callanalyticscategory*		
GetCallAnalyticsJob	Accorde l'autorisation de renvoyer des informations sur une tâche d'analyse des appels	Lecture	callanalyticsjob*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMedicalScribeJob	Octroie l'autorisation de renvoyer des informations sur une tâche de transcription médicale.	Lecture	medicalscribejob*		
GetMedicalScribeStream	Accorde l'autorisation d'obtenir des informations sur la session de AWS HealthScribe streaming spécifiée	Lecture			
GetMedicalTranscriptionJob	Accorde l'autorisation de retourner des informations sur une tâche de transcription médicale	Read	medicaltranscriptionjob*		
GetMedicalVocabulary	Accorde l'autorisation d'obtenir des informations sur un vocabulaire médical	Read	medicalvocabulary*		
GetTranscriptionJob	Accorde l'autorisation de renvoyer des informations sur une tâche de transcription	Read	transcriptionjob*		
GetVocabulary	Accorde l'autorisation d'obtenir des informations sur un vocabulaire	Read	vocabulary*		
GetVocabularyFilter	Accorde l'autorisation d'obtenir des informations sur un filtre de vocabulaire	Read	vocabularyfilter*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCallAnalyticsCategories	Accorde l'autorisation de répertorier les catégories d'analyse des appels qui ont été créées	Liste			
ListCallAnalyticsJobs	Accorde l'autorisation de répertorier les tâches d'analytique des appels avec le statut spécifié	Liste			
ListLanguageModels	Accorde l'autorisation de répertorier les modèles de langue personnalisés	List			
ListMedicalScribeJobs	Octroie l'autorisation de répertorier les tâches de transcription médicale avec le statut spécifié.	List			
ListMedicalTranscriptionJobs	Accorde l'autorisation de répertorier les tâches de transcription médicale avec le statut spécifié	Liste			
ListMedicalVocabularies	Accorde l'autorisation de renvoyer une liste de vocabulaires médicaux correspondant aux critères spécifiés. Si aucun critère n'est spécifié, renvoie l'ensemble de la liste des vocabulaires	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture			
ListTranscriptionJobs	Accorde l'autorisation de répertorier les tâches de transcription avec le statut spécifié	Liste			
ListVocabularies	Accorde l'autorisation de renvoyer une liste de vocabulaires correspondant aux critères spécifiés. Si aucun critère n'est spécifié, renvoie l'ensemble de la liste des vocabulaires	Liste			
ListVocabularyFilters	Accorde l'autorisation de renvoyer une liste de filtres de vocabulaire correspondant aux critères spécifiés. Si aucun critère n'est spécifié, renvoie au maximum 5 filtres de vocabulaire	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartCallAnalyticsJob	Accorde l'autorisation de démarrer une tâche d'analyse asynchrone qui non seulement transcrit l'enregistrement audio d'un appelant et d'un agent, mais renvoie également des informations supplémentaires	Écrire		transcribe:OutputEncryptionKMSKeyId transcribe:OutputLocation aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartCallAnalyticsStreamTranscription	Accorde l'autorisation de démarrer un protocole où l'audio est diffusé en continu vers Transcribe Call Analytics et les résultats de la transcription sont diffusés sur votre application	Écrire			
StartCallAnalyticsStreamTranscriptionWebSocket	Autorise le lancement d'un fichier WebSocket où le son est diffusé vers Transcribe Call Analytics et où les résultats de la transcription sont transmis à votre application	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMedicalScribeJob	Octroie l'autorisation de démarrer une tâche asynchrone pour transcrire les conversations patient-clinicien et générer des notes cliniques.	Écrire		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalScribeStream	Autorise le lancement d'un HTTP2 flux bidirectionnel dans lequel le son est diffusé AWS HealthScribe et les résultats de la transcription sont transmis à votre application	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMedicalStreamTranscription	Accorde l'autorisation de démarrer un protocole où l'audio est diffusé en continu vers Transcribe Medical et les résultats de la transcription sont diffusés sur votre application	Écrire			
StartMedicalStreamTranscriptionWebSocket	Autorise le lancement d'une application WebSocket où le son est diffusé vers Transcribe Medical et les résultats de la transcription sont transmis à votre application	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartMedicalTranscriptionJob	Accorde l'autorisation de démarrer une tâche asynchrone pour transcrire le discours médical en texte	Écrire		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
StartStreamTranscription	Autorise le lancement d'un HTTP2 flux bidirectionnel pour transcrire la parole en texte en temps réel	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartStreamTranscriptionWebSocket	Accorde l'autorisation de démarrer un flux websocket pour transcrire la parole en texte en temps réel	Écriture			
StartTranscriptionJob	Accorde l'autorisation de démarrer une tâche asynchrone pour transcrire la parole en texte	Écrire		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Balisage		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource avec une clé donnée	Identification		aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateCallAnalyticsCategory	Accorde l'autorisation de mettre à jour la catégorie d'analyse des appels avec de nouvelles valeurs L' UpdateCallAnalyticsCategory opération remplace toutes les informations existantes par les valeurs que vous fournissez dans la demande	Écrire	callanalyticscategory*		
UpdateMedicalVocabulary	Accorde l'autorisation de mettre à jour un vocabulaire médical existant avec de nouvelles valeurs. L' UpdateMedicalVocabulary opération remplace toutes les informations existantes par les valeurs que vous fournissez dans la demande	Écrire	medicalvocabulary*		s3:GetObject
UpdateVocabulary	Accorde l'autorisation de mettre à jour un vocabulaire existant avec de nouvelles valeurs. L' UpdateVocabulary opération remplace toutes les informations existantes par les valeurs que vous fournissez dans la demande	Écrire	vocabulary*		s3:GetObject

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateVocabularyFilter	Accorde l'autorisation de mettre à jour un filtre de vocabulaire existant avec de nouvelles valeurs. L'UpdateVocabularyFilter opération remplace toutes les informations existantes par les valeurs que vous fournissez dans la demande	Écrire	vocabularyfilter*		s3:GetObject

Types de ressources définis par Amazon Transcribe

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l'`Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
transcriptionjob	`arn:${Partition}:transcribe:${Region}:${Account}:transcription-job/${JobName}`	aws:ResourceTag/${TagKey}
vocabulary	`arn:${Partition}:transcribe:${Region}:${Account}:vocabulary/${VocabularyName}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
vocabularyfilter	arn:${Partition}:transcribe:${Region}:${Account}:vocabulary-filter/${VocabularyFilterName}	aws:ResourceTag/${TagKey}
languagemodel	arn:${Partition}:transcribe:${Region}:${Account}:language-model/${ModelName}	aws:ResourceTag/${TagKey}
medicaltranscriptionjob	arn:${Partition}:transcribe:${Region}:${Account}:medical-transcription-job/${JobName}	aws:ResourceTag/${TagKey}
medicalvocabulary	arn:${Partition}:transcribe:${Region}:${Account}:medical-vocabulary/${VocabularyName}	aws:ResourceTag/${TagKey}
callanalyticsjob	arn:${Partition}:transcribe:${Region}:${Account}:analytics/${JobName}	aws:ResourceTag/${TagKey}
callanalyticscategory	arn:${Partition}:transcribe:${Region}:${Account}:analytics-category/${CategoryName}	aws:ResourceTag/${TagKey}
medicalscribejob	arn:${Partition}:transcribe:${Region}:${Account}:medical-scribe-job/${JobName}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Transcribe

Amazon Transcribe définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une stratégie IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en exigeant des valeurs d'identification présentes dans une demande de création de ressources	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence d'identifications obligatoires dans la demande	ArrayOfString
transcribe:OutputBucketName	Filtre l'accès en fonction du nom du compartiment de sortie inclus dans la demande	String
transcribe:OutputEncryptionKMSKeyId	Filtre l'accès en fonction de l'identifiant de clé KMS inclus dans la demande, fourni sous la forme d'un ARN de clé KMS	String
transcribe:OutputKey	Filtre l'accès en fonction de la clé de sortie incluse dans la demande	String
transcribe:OutputLocation	Filtre l'accès en fonction de l'emplacement de sortie incluse dans la demande	String

Actions, ressources et clés de condition pour AWS Transfer Family

AWS Transfer Family (préfixe de service :`transfer`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.

- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Transfer Family
- Types de ressources définis par AWS Transfer Family
- Clés de condition pour AWS Transfer Family

Actions définies par AWS Transfer Family

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAccess	Accorde l'autorisation d'ajouter un accès associé à un serveur	Écrire	server*		iam:PassRole
CreateAgreement	Accorde l'autorisation d'ajouter un accord associé à un serveur	Écrire	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CreateConnector	Accorde l'autorisation de créer un connecteur	Écrire	profile		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transfer:RequestConnectorProtocol	
CreateProfile	Accorde l'autorisation de créer un profil	Écrire		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateServer	Accorde l'autorisation de créer un serveur	Écriture		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transfer:RequestServerEndpointType transfer:RequestServerDomain transfer:RequestServerProtocols	iam:PassRole
CreateUser	Accorde l'autorisation d'ajouter un utilisateur associé à un serveur	Écrire	server*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateWebApp	Accorde l'autorisation de créer une application Web	Écrire		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole
CreateWorkflow	Accorde l'autorisation de créer un flux de travail.	Écrire		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccess	Accorde l'autorisation de supprimer un accès	Écrire	server*		
DeleteAgreement	Accorde l'autorisation de supprimer un accord	Écrire	agreement*		
DeleteCertificate	Accorde l'autorisation de supprimer un certificat	Écrire	certificate*		
DeleteConnector	Accorde l'autorisation de supprimer un connecteur	Écrire	connector*		
DeleteHostKey	Accorde l'autorisation de supprimer une clé d'hôte associée à un serveur	Écrire	host-key*		
DeleteProfile	Accorde l'autorisation de supprimer un profil	Écrire	profile*		
DeleteServer	Accorde l'autorisation de supprimer un serveur	Écriture	server*		
DeleteSshPublicKey	Accorde l'autorisation de supprimer une clé publique SSH d'un utilisateur	Écriture	user*		
DeleteUser	Accorde l'autorisation de supprimer un utilisateur associé à un serveur	Écrire	user*		
DeleteWebApp	Autorise la suppression de l'application Web	Écrire	webapp*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteWebAppCustomization	Autorise la suppression de la personnalisation de l'application Web	Écrire	webapp*		
DeleteWorkflow	Accorde l'autorisation de supprimer un flux de travail.	Écrire	workflow*		
DescribeAccess	Accorde l'autorisation de décrire un accès associé à un serveur	Lecture	server*		
DescribeAgreement	Accorde l'autorisation de décrire un accord associé à un serveur	Lecture	agreement*		
DescribeCertificate	Accorde l'autorisation de décrire un certificat	Lecture	certificate*		
DescribeConnector	Accorde l'autorisation de décrire un connecteur	Lecture	connector*		
DescribeExecution	Accorde l'autorisation de décrire une exécution associée à un flux de travail	Lecture	workflow*		
DescribeHostKey	Accorde l'autorisation de décrire une clé d'hôte associée à un serveur	Lecture	host-key*		
DescribeProfile	Accorde l'autorisation de décrire un profil	Lecture	profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeSecurityPolicy	Accorde l'autorisation de décrire une politique de sécurité	Lecture			
DescribeServer	Accorde l'autorisation de décrire un serveur	Lecture	server*		
DescribeUser	Accorde l'autorisation de décrire un utilisateur associé à un serveur	Lecture	user*		
DescribeWebApp	Accorde l'autorisation de décrire une application Web	Lecture	webapp*		
DescribeWebAppCustomization	Accorde l'autorisation de décrire la personnalisation d'une application Web	Lecture	webapp*		
DescribeWorkflow	Accorde l'autorisation de décrire un flux de travail	Lecture	workflow*		
ImportCertificate	Accorde l'autorisation d'ajouter un certificat	Écrire		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ImportHostKey	Accorde l'autorisation d'ajouter une clé d'hôte à un serveur	Écrire	server*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
ImportSshPublicKey	Accorde l'autorisation d'ajouter une clé publique SSH à un utilisateur	Écrire	user*		
ListAccesses	Accorde l'autorisation de répertorier des accès	Lecture	server*		
ListAgreements	Accorde l'autorisation de répertorier des accords	Lecture	server*		
ListCertificates	Accorde l'autorisation de répertorier les certificats	Lecture			
ListConnectors	Accorde l'autorisation de répertorier les connecteurs	Lecture			
ListExecutions	Accorde l'autorisation de répertorier les exécutions associées à un flux de travail	Lecture	workflow*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListFileTransferResults	Accorde l'autorisation de répertorier les statuts de transfert de fichiers pour les connecteurs	Lecture	connector*		
ListHostKeys	Accorde l'autorisation de répertorier les clés d'hôte associées à un serveur	Lecture	server*		
ListProfiles	Accorde l'autorisation de répertorier des profils	Lecture			
ListSecurityPolicies	Accorde l'autorisation de répertorier les politiques de sécurité	Liste			
ListServers	Accorde l'autorisation de répertorier les serveurs	List			
ListTagsForResource	Accorde l'autorisation de répertorier les tags d'une ressource AWS Transfer Family	Lecture	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListUsers	Accorde l'autorisation de répertorier les utilisateurs associés à un serveur	List	server*		
ListWebApps	Accorde l'autorisation de répertorier les applications Web	List			
ListWorkflows	Accorde l'autorisation de répertorier des flux de travail	List			
SendWorkflowStepState	Accorde l'autorisation d'envoyer un rappel pour des étapes personnalisées asynchrones	Écrire	workflow*		
StartDirectoryListing	Accorde l'autorisation de lancer une opération de liste sur un serveur distant à l'aide d'un connecteur	Écrire	connector*		
StartFileTransfer	Accorde l'autorisation d'initier un transfert de fichier connecteur	Écrire	connector*		
StartRemoteDelete	Autorise le lancement d'une opération de suppression du connecteur sur un serveur distant	Écrire	connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartRemoteMove	Autorise le lancement d'une opération de déplacement de connecteur sur un serveur distant	Écrire	connector*		
StartServer	Accorde l'autorisation de démarrer un serveur	Écriture	server*		
StopServer	Accorde l'autorisation d'arrêter un serveur	Écrire	server*		
TagResource	Accorde l'autorisation de baliser une ressource AWS Transfer Family	Identification	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConnection	Octroie l'autorisation de tester la connexion d'un connecteur à un serveur distant.	Écrire	connector*		
TestIdentityProvider	Accorde l'autorisation de tester le fournisseur d'identité personnalisé d'un serveur	Lecture	user*		
UntagResource	Accorde l'autorisation de supprimer le tag d'une ressource AWS Transfer Family	Identification	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
UpdateAccess	Accorde l'autorisation de mettre à jour un accès	Écrire			iam:PassRole
UpdateAgreement	Accorde l'autorisation de mettre à jour un accord	Écrire	agreement*		iam:PassRole
UpdateCertificate	Accorde l'autorisation de mettre à jour un certificat	Écrire	certificate*		
UpdateConnector	Accorde l'autorisation de mettre à jour un connecteur	Écrire	connector*		iam:PassRole
			profile		
UpdateHostKey	Accorde l'autorisation de mettre à jour une clé d'hôte	Écrire	host-key*		
UpdateProfile	Accorde l'autorisation de mettre à jour un profil	Écrire	profile*		
UpdateServer	Accorde l'autorisation de mettre à jour la configuration d'un serveur	Écriture	server*		iam:PassRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				transfer:RequestServerEndpointType transfer:RequestServerProtocols	
UpdateUser	Accorde l'autorisation de mettre à jour la configuration d'un utilisateur	Écrire	user*		iam:PassRole
UpdateWebApp	Accorde l'autorisation de mettre à jour la configuration d'une application Web	Écrire	webapp*		iam:PassRole
UpdateWebAppCustomization	Accorde l'autorisation de mettre à jour la configuration d'une application Web personnalisée	Écrire	webapp*		iam:PassRole

Types de ressources définis par AWS Transfer Family

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
user	arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}	aws:ResourceTag/${TagKey}
server	arn:${Partition}:transfer:${Region}:${Account}:server/${ServerId}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:transfer:${Region}:${Account}:workflow/${WorkflowId}	aws:ResourceTag/${TagKey}
certificate	arn:${Partition}:transfer:${Region}:${Account}:certificate/${CertificateId}	aws:ResourceTag/${TagKey}
connector	arn:${Partition}:transfer:${Region}:${Account}:connector/${ConnectorId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:transfer:${Region}:${Account}:profile/${ProfileId}	aws:ResourceTag/${TagKey}
agreement	arn:${Partition}:transfer:${Region}:${Account}:agreement/${ServerId}/${AgreementId}	aws:ResourceTag/${TagKey}
host-key	arn:${Partition}:transfer:${Region}:${Account}:host-key/${ServerId}/${HostKeyId}	aws:ResourceTag/${TagKey}
webapp	arn:${Partition}:transfer:${Region}:${Account}:webapp/${WebAppId}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Transfer Family

AWS Transfer Family définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions

d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
transfer:RequestConnectorProtocol	Filtre l'accès par le protocole de connecteur transmis dans la demande	String
transfer:RequestServerDomain	Filtre l'accès en fonction du domaine de stockage transmis dans la demande	String
transfer:RequestServerEndpointType	Filtre l'accès en fonction du type de point de terminaison transmis dans la demande	String
transfer:RequestServerProtocols	Filtre l'accès par les protocoles du serveur transmis dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Transform

AWS Transform (préfixe de service :`transform`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Transform
- Types de ressources définis par AWS Transform
- Clés de condition pour AWS Transform

Actions définies par AWS Transform

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate Connector Resource [autorisation uniquement]	Accorde l'autorisation d'invoquer Associate ConnectorResource sur AWS Transform	Écrire	connector *		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateProfile [autorisation uniquement]	Accorde l'autorisation d'invoquer CreateProfile sur AWS Transform	Écrire	profile*		
DeleteAgentRuntimeConfiguration [autorisation uniquement]	Accorde l'autorisation d'invoquer DeleteAgentRuntimeConfiguration sur AWS Transform	Écrire			
DeleteConnector [autorisation uniquement]	Accorde l'autorisation d'invoquer DeleteConnector sur AWS Transform	Écrire	connector*		
DeleteProfile [autorisation uniquement]	Accorde l'autorisation d'invoquer DeleteProfile sur AWS Transform	Écrire	profile*		
GetAccountSettings [autorisation uniquement]	Accorde l'autorisation d'invoquer GetAccountSettings sur AWS Transform	Lecture			
GetAgent [autorisation uniquement]	Accorde l'autorisation d'invoquer GetAgent sur AWS Transform	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAgentRuntimeConfiguration [autorisation uniquement]	Accorde l'autorisation d'invoquer GetAgentRuntimeConfiguration sur AWS Transform	Lecture			
GetConnector [autorisation uniquement]	Accorde l'autorisation d'invoquer GetConnector sur AWS Transform	Lecture	connector*		
ListAgents [autorisation uniquement]	Accorde l'autorisation d'invoquer ListAgents sur AWS Transform	Lecture			
ListConnectors [autorisation uniquement]	Accorde l'autorisation d'invoquer ListConnectors sur AWS Transform	List			
ListProfiles [autorisation uniquement]	Accorde l'autorisation d'invoquer ListProfiles sur AWS Transform	List			
ListTagsForResource [autorisation uniquement]	Accorde l'autorisation d'invoquer ListTagsForResource sur AWS Transform	Lecture	connector*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutAgentRuntimeConfiguration [autorisation uniquement]	Accorde l'autorisation d'invoquer PutAgentRuntimeConfiguration sur AWS Transform	Écrire			
RejectConnector [autorisation uniquement]	Accorde l'autorisation d'invoquer RejectConnector sur AWS Transform	Écrire	connector*		
TagResource [autorisation uniquement]	Accorde l'autorisation d'invoquer TagResource sur AWS Transform	Identification	connector*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [autorisation uniquement]	Accorde l'autorisation d'invoquer UntagResource sur AWS Transform	Identification	connector*		
				aws:TagKeys	
UpdateAccountSettings [autorisation uniquement]	Accorde l'autorisation d'invoquer UpdateAccountSettings sur AWS Transform	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAgentAccess [autorisation uniquement]	Accorde l'autorisation d'invoquer UpdateAgentAccess sur AWS Transform	Écrire			
UpdateProfile [autorisation uniquement]	Accorde l'autorisation d'invoquer UpdateProfile sur AWS Transform	Écrire	profile*		

Types de ressources définis par AWS Transform

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
profile	`arn:${Partition}:transform:${Region}:${Account}:profile/${Identifier}`	
connector	`arn:${Partition}:transform:${Region}:${Account}:connector/${WorkspaceId}/${ConnectorId}`	

Clés de condition pour AWS Transform

AWS Transform définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Transform custom

AWS Transform custom (préfixe de service :`transform-custom`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Transform custom
- Types de ressources définis par AWS Transform custom
- Clés de condition pour AWS Transform custom

Actions définies par AWS Transform custom

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CompleteTransformationPackageUpload	Accorde l'autorisation d'invoquer CompleteTransformationPackageUpload sur AWS Transform custom	Écrire	package*		
				aws:ResourceTag/${TagKey}	
ConverseStream	Accorde l'autorisation d'invoquer ConverseStream sur AWS Transform custom	Écrire			
CreateCampaign	Accorde l'autorisation d'invoquer CreateCampaign sur AWS Transform custom	Écrire	campaign*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTransformati	Accorde l'autorisation d'invoquer CreateTransformati	Écrire	package*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
onPackageUrl	onPackageUrl sur AWS Transform custom			aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteCampaign	Accorde l'autorisation d'invoquer DeleteCampaign sur AWS Transform custom	Écrire	campaign*		
				aws:ResourceTag/${TagKey}	
DeleteKnowledgeItem	Accorde l'autorisation d'invoquer DeleteKnowledgeItem sur AWS Transform custom	Écrire	knowledge-item*		
				aws:ResourceTag/${TagKey}	
DeleteTransformationPackage	Accorde l'autorisation d'invoquer DeleteTransformationPackage sur AWS Transform custom	Écrire	package*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExecuteTransformation	Accorde l'autorisation d'invoquer ExecuteTransformation sur AWS Transform custom	Écrire	package*		
				aws:ResourceTag/${TagKey}	
GetCampaign	Accorde l'autorisation d'invoquer GetCampaign sur AWS Transform custom	Lecture	campaign*		
				aws:ResourceTag/${TagKey}	
GetKnowledgeItem	Accorde l'autorisation d'invoquer GetKnowledgeItem sur AWS Transform custom	Lecture	knowledge-item*		
				aws:ResourceTag/${TagKey}	
GetTransformationPackageUrl	Accorde l'autorisation d'invoquer GetTransformationPackageUrl sur AWS Transform custom	Lecture	package*		
				aws:ResourceTag/${TagKey}	
ListCampaignRepositories	Accorde l'autorisation d'invoquer ListCampaignRepositories sur AWS Transform custom	Lecture	campaign*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListCampaigns	Accorde l'autorisation d'invoquer ListCampaign sur AWS Transform custom	List			
ListKnowledgeItems	Accorde l'autorisation d'invoquer ListKnowledgeItems sur AWS Transform custom	List			
ListTagsForResource	Accorde l'autorisation d'invoquer ListTagsForResource sur AWS Transform custom	Lecture			
ListTransformationPackageMetadata	Accorde l'autorisation d'invoquer ListTransformationPackageMetadata sur AWS Transform custom	List			
TagResource	Accorde l'autorisation d'invoquer TagResource sur AWS Transform custom	Identification	campaign		
			knowledge-item		
			package		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'invoquer UntagResource sur AWS Transform custom	Identification	campaign		
			knowledge-item		
			package		
				aws:TagKeys	
UpdateCampaign	Accorde l'autorisation d'invoquer UpdateCampaign sur AWS Transform custom	Écrire	campaign*		
				aws:ResourceTag/${TagKey}	
UpdateCampaignRepositoryStatus	Accorde l'autorisation d'invoquer UpdateCampaignRepositories sur AWS Transform custom	Écrire	campaign*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateKnowledgeItemConfiguration	Accorde l'autorisation d'invoquer UpdateKnowledgeItemConfiguration sur AWS Transform custom	Écrire	package*		
				aws:ResourceTag/${TagKey}	
UpdateKnowledgeItemStatus	Accorde l'autorisation d'invoquer UpdateKnowledgeItemStatus sur AWS Transform custom	Écrire	knowledge-item*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS Transform custom

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
campaign	`arn:${Partition}:transform-custom:${Region}:${Account}:campaign/${Name}`	aws:ResourceTag/${TagKey}
knowledge-item	`arn:${Partition}:transform-custom:${Region}:${Account}:package/${Transfo`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
	`rmationPackageName}/knowledge-item/${Id}`	
package	`arn:${Partition}:transform-custom:${Region}:${Account}:package/${Name}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Transform custom

AWS Transform custom définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon Translate

Amazon Translate (préfixe de service : `translate`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Translate
- Types de ressources définis par Amazon Translate
- Clés de condition pour Amazon Translate

Actions définies par Amazon Translate

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateParallelData	Accorde l'autorisation de créer des données en parallèle	Écriture	parallel-data		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteParallelData	Accorde l'autorisation de supprimer des données en parallèle	Écriture	parallel-data		
DeleteTerminology	Accorde l'autorisation de supprimer une terminologie	Écriture	terminology		
DescribeTextTranslationJob	Accorde l'autorisation d'obtenir les propriétés associées à une tâche asynchrone de traduction par lots	Lecture			
GetParallelData	Accorde l'autorisation d'obtenir des données en parallèle	Lecture	parallel-data		
GetTerminology	Accorde l'autorisation de récupérer une terminologie	Lecture	terminology		
ImportTerminology	Accorde l'autorisation de créer ou de mettre à jour une terminologie, selon qu'un groupe existe déjà ou pas pour le nom de terminologie donné	Écrire	terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListLanguages	Accorde l'autorisation de répertorier les langues prises en charge	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListParallelData	Accorde l'autorisation de répertorier les données en parallèle associées à votre compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	parallel-data		
			terminology		
ListTerminologies	Accorde l'autorisation de répertorier les terminologies associées à votre compte	Liste			
ListTextTranslationJobs	Accorde l'autorisation de répertorier les tâches de traduction par lots que vous avez soumises	Liste			
StartTextTranslationJob	Accorde l'autorisation de démarrer une tâche asynchrone de traduction par lots Les tâches de traduction par lots peuvent être utilisées pour traduire de grands volumes de texte de plusieurs documents à la fois.	Écriture	parallel-data		
			terminology		
StopTextTranslationJob	Accorde l'autorisation d'arrêter une tâche asynchrone de traduction par lots	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'identificationr une ressource avec des paires de valeurs clés données	Identification	parallel-data		
			terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
TranslateDocument	Accorde l'autorisation de traduire un document d'une langue source vers une langue cible.	Lecture	terminology		
TranslateText	Accorde l'autorisation de traduire du texte d'une langue source vers une langue cible	Lecture	parallel-data		
			terminology		
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource avec une clé donnée	Identification	parallel-data		
			terminology		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateParallelData	Accorde l'autorisation de mettre à jour des données en parallèle existantes	Écriture	parallel-data		

Types de ressources définis par Amazon Translate

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
terminology	`arn:${Partition}:translate:${Region}:${Account}:terminology/${ResourceName}`	aws:ResourceTag/${TagKey}
parallel-data	`arn:${Partition}:translate:${Region}:${Account}:parallel-data/${ResourceName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Translate

Amazon Translate définit les clés de condition suivantes qui peuvent être utilisées dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en exigeant des valeurs d'identification présentes dans une demande de création de ressources	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence d'identifications obligatoires dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS Trusted Advisor

AWS Trusted Advisor (préfixe de service :`trustedadvisor`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Trusted Advisor
- Types de ressources définis par AWS Trusted Advisor
- Clés de condition pour AWS Trusted Advisor

Actions définies par AWS Trusted Advisor

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération

dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

> **Note**
>
> La description de la politique IAM Trusted Advisor s'applique uniquement à la console Trusted Advisor. Si vous souhaitez gérer l'accès programmatique à Trusted Advisor, utilisez les opérations Trusted Advisor dans l' AWS Support API.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchUpdateRecommendationResourceExclusion	Accorde l'autorisation de mettre à jour un ou plusieurs statuts d'exclusion pour une liste de ressources de recommandation	Écrire			
CreateEngagement	Accorde l'autorisation de créer un engagement	Écrire			
CreateEngagementAttachment	Accorde l'autorisation de créer la pièce jointe d'un engagement	Écrire			
CreateEngagementCommunication	Accorde l'autorisation de créer la communication d'un engagement	Écrire			
DeleteNotificationConfigurationForDelegatedAdmin	Accorde l'autorisation au compte de gestion de l'organisation de supprimer les préférences de notification par e-mail d'un compte administr	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	ateur délégué pour Trusted Advisor Priority				
DescribeAccount [autorisation uniquement]	Permet de consulter le AWS Support plan et les différentes préférences de AWS Trusted Advisor	Lecture			
DescribeAccountAccess [autorisation uniquement]	Accorde l'autorisation de voir si AWS Trusted Advisor Compte AWS a activé ou désactivé	Lecture			
DescribeCheckItems	Accorde l'autorisation d'afficher les détails des éléments de vérification	Lecture	checks*		
DescribeCheckRefreshStatuses	Accorde l'autorisation de consulter les statuts d'actualisation des contrôles AWS Trusted Advisor	Lecture	checks*		
DescribeCheckStatusHistoryChanges [autorisation uniquement]	Octroie l'autorisation de consulter les résultats et les statuts modifiés pour les vérifications effectuées au cours des 30 derniers jours	Lecture	checks*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCheckSummaries	Accorde l'autorisation de consulter les résumés AWS des chèques de Trusted Advisor	Lecture	checks*		
DescribeChecks	Accorde l'autorisation de consulter les détails des contrôles AWS Trusted Advisor	Lecture			
DescribeNotificationConfigurations	Accorde l'autorisation d'obtenir vos préférences de notification par e-mail pour Trusted Advisor Priority	Lecture			
DescribeNotificationPreferences [autorisation uniquement]	Accorde l'autorisation de consulter les préférences de notification pour Compte AWS	Lecture			
DescribeOrganization [autorisation uniquement]	Accorde l'autorisation de voir s'il Compte AWS répond aux exigences pour activer la fonctionnalité d'affichage organisationnel	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeOrganizationAccounts [autorisation uniquement]	Accorde l'autorisation de consulter les AWS comptes associés qui se trouvent dans l'organisation	Lecture			
DescribeReports [autorisation uniquement]	Accorde l'autorisation d'afficher les détails des rapports d'affichage organisationnel, tels que le nom, l'exécution, la date de création, l'état et le format du rapport	Lecture			
DescribeRisk	Accorde l'autorisation de consulter les détails des risques dans AWS Trusted Advisor Priority	Lecture			
DescribeRiskResources	Accorde l'autorisation de consulter les ressources affectées par un risque dans AWS Trusted Advisor Priority	Lecture			
DescribeRisks	Permet de visualiser les risques dans AWS Trusted Advisor Priority	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeServiceMetadata [autorisation uniquement]	Accorde l'autorisation de consulter les informations relatives aux rapports d'affichage organisationnels, telles que les Régions AWS catégories de vérifications, les noms des vérifications et les statuts des ressources	Lecture			
DownloadRisk	Autorise le téléchargement d'un fichier contenant des informations détaillées sur le risque dans AWS Trusted Advisor Priority	Lecture			
ExcludeCheckItems [autorisation uniquement]	Autorise l'exclusion des recommandations pour les contrôles AWS Trusted Advisor	Écrire	checks*		
GenerateReport [autorisation uniquement]	Accorde l'autorisation de créer un rapport pour les contrôles AWS Trusted Advisor dans votre organisation	Écrire			
GetEngagement	Accorde l'autorisation d'afficher un engagement	Lecture			
GetEngagementAttachment	Accorde l'autorisation d'afficher la pièce jointe d'un engagement	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetEngagementType	Accorde l'autorisation d'afficher le type d'un engagement spécifique	Lecture			
GetOrganizationRecommendation	Accorde l'autorisation d'obtenir une recommandation spécifique au sein de AWS l'organisation d'une organisation. Cette API ne prend en charge que les recommandations prioritaires.	Lecture			
GetRecommendation	Octroie l'autorisation d'obtenir une recommandation spécifique.	Lecture			
IncludeCheckItems [autorisation uniquement]	Autorise l'inclusion de recommandations pour les contrôles AWS Trusted Advisor	Écrire	checks*		
ListAccountsForParent [autorisation uniquement]	Accorde l'autorisation de consulter, dans la console Trusted Advisor, tous les comptes d'une AWS organisation qui sont contenus par une racine ou une unité organisationnelle (UO)	Lecture			
ListChecks	Octroie l'autorisation de répertorier un ensemble filtrable de vérifications.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListEngagementCommunications	Accorde l'autorisation d'afficher toutes les communications d'un engagement	Lecture			
ListEngagementTypes	Accorde l'autorisation d'afficher tous les types d'engagement	Lecture			
ListEngagements	Accorde l'autorisation d'afficher tous les engagements	Lecture			
ListOrganizationRecommendationAccounts	Accorde l'autorisation de répertorier les comptes propriétaires des ressources pour une recommandation globale d' AWS organisation. Cette API prend uniquement en charge les recommandations prioritaires.	List			
ListOrganizationRecommendationResources	Accorde l'autorisation de répertorier les ressources d'une recommandation au sein d'une AWS organisation. Cette API prend uniquement en charge les recommandations prioritaires.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOrganizationRecommendations	Accorde l'autorisation de répertorier un ensemble filtrable de recommandations au sein d'une AWS organisation. Cette API prend uniquement en charge les recommandations prioritaires.	List			
ListOrganizationalUnitsForParent [autorisation uniquement]	Accorde l'autorisation d'afficher, dans la console Trusted Advisor, toutes les unités organisationnelles (OUs) d'une unité organisationnelle parent ou racine	Lecture			
ListRecommendationResources	Octroie l'autorisation de répertorier les ressources d'une recommandation.	List			
ListRecommendations	Octroie l'autorisation de répertorier un ensemble filtrable de recommandations.	List			
ListRoots [autorisation uniquement]	Autorise l'affichage, dans la console Trusted Advisor, de toutes les racines définies dans une AWS organisation	Lecture			
RefreshCheck	Accorde l'autorisation d'actualiser un check AWS Trusted Advisor	Écrire	checks*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
SetAccountAccess [autorisation uniquement]	Accorde l'autorisation d'activer ou de désactiver AWS Trusted Advisor pour le compte	Écrire			
SetOrganizationAccess [autorisation uniquement]	Accorde l'autorisation d'activer la fonctionnalité d'affichage organisationnel pour AWS Trusted Advisor	Écrire			
UpdateEngagement	Octroie l'autorisation de mettre à jour les détails d'un engagement.	Écrire			
UpdateEngagementStatus	Accorde l'autorisation de mettre à jour le statut d'un engagement	Écrire			
UpdateNotificationConfigurations	Accorde l'autorisation de créer ou mettre à jour vos préférences de notification par e-mail pour Trusted Advisor Priority	Écrire			
UpdateNotificationPreferences [autorisation uniquement]	Autorise la mise à jour des préférences de notification pour AWS Trusted Advisor	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateOrganizationRecommendationLifecycle	Accorde l'autorisation de mettre à jour le cycle de vie d'une recommandation au sein d'une AWS organisation. Cette API prend uniquement en charge les recommandations prioritaires.	Écrire			
UpdateRecommendationLifecycle	Octroie l'autorisation de mettre à jour le cycle de vie d'une recommandation. Cette API prend uniquement en charge les recommandations prioritaires.	Écrire			
UpdateRiskStatus	Autorise la mise à jour de l'état du risque dans AWS Trusted Advisor Priority	Écrire			

Types de ressources définis par AWS Trusted Advisor

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

> **Note**
>
> L'ARN du type de ressource de vérification ne doit pas inclure de région. Dans le format, au lieu de « ${Region} », utilisez un « * » ou la politique ne fonctionnera pas correctement.

Types de ressources	ARN	Clés de condition
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

Clés de condition pour AWS Trusted Advisor

Trusted Advisor ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour la personnalisation de AWS l'expérience utilisateur

AWS La personnalisation de l'expérience utilisateur (préfixe de service :`uxc`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par la personnalisation de AWS l'expérience utilisateur

- Types de ressources définis par la personnalisation de AWS l'expérience utilisateur
- Clés de condition pour la personnalisation de l'expérience AWS utilisateur

Actions définies par la personnalisation de AWS l'expérience utilisateur

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccountColor	Autorise la suppression du paramètre de couleur du compte	Écrire			
GetAccountColor	Accorde l'autorisation de récupérer la couleur du compte pour un compte donné	Lecture			
GetAccountCustomizations	Accorde l'autorisation de récupérer les personnalisations du compte	Lecture			
ListServices	Accorde l'autorisation de répertorier les services disponibles	Lecture			
PutAccountColor	Accorde l'autorisation de définir la couleur du compte	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAccountCustomizations	Accorde l'autorisation de mettre à jour les personnalisations du compte	Écrire			

Types de ressources définis par la personnalisation de AWS l'expérience utilisateur

AWS La personnalisation de l'expérience utilisateur ne permet pas de spécifier un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à la personnalisation de AWS l'expérience utilisateur, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour la personnalisation de l'expérience AWS utilisateur

La personnalisation de l'expérience utilisateur (UXC) ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les notifications AWS utilisateur

AWS Les notifications utilisateur (préfixe de service :`notifications`) fournissent les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les notifications AWS utilisateur
- Types de ressources définis par les notifications AWS utilisateur
- Clés de condition pour les notifications aux AWS utilisateurs

Actions définies par les notifications AWS utilisateur

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions

dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateChannel	Accorde l'autorisation d'associer une nouvelle chaîne à une chaîne en particulier NotificationConfiguration	Écrire	NotificationConfiguration*		
AssociateManagedNotificationAccountContact	Accorde l'autorisation d'associer un contact du compte à une configuration de notification gérée particulière	Écrire	ManagedNotificationConfiguration*		
AssociateManagedNotificationAdditionalChannel	Accorde l'autorisation d'associer un canal à une configuration de notification gérée particulière	Écrire	ManagedNotificationConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateOrganizationalUnit	Accorde l'autorisation d'associer une unité organisationnelle à une configuration de notification particulière	Écrire	NotificationConfiguration*		
CreateEventRule	Accorde l'autorisation d'en créer un nouveau EventRule, en l'associant à un NotificationConfiguration	Écrire			
CreateNotificationConfiguration	Accorde l'autorisation de créer un NotificationConfiguration	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEventRule	Accorde l'autorisation de supprimer un EventRule	Écrire	EventRule*		
DeleteNotificationConfiguration	Accorde l'autorisation de supprimer un NotificationConfiguration	Écrire	NotificationConfiguration*		
DeregisterNotificationHub	Accorde l'autorisation de désenregistrer un NotificationHub	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisableNotificationsAccessForOrganization	Accorde l'autorisation de désactiver Service Trust pour les notifications AWS utilisateur	Gestion des autorisations			organizations:DisableAWSServiceAccess
DisassociateChannel	Accorde l'autorisation de supprimer une chaîne d'un NotificationConfiguration	Écrire	NotificationConfiguration*		
DisassociateManagedNotificationAccountContact	Accorde l'autorisation de supprimer un contact du compte d'une configuration de notification gérée	Écrire	ManagedNotificationConfiguration*		
DisassociateManagedNotificationAdditionalChannel	Accorde l'autorisation de supprimer un canal d'une configuration de notification gérée	Écrire	ManagedNotificationConfiguration*		
DisassociateOrganizationalUnit	Accorde l'autorisation de dissocier une unité organisationnelle d'une configuration de notification particulière	Écrire	NotificationConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableNotificationsAccessForOrganization	Accorde l'autorisation d'activer Service Trust pour les notifications AWS utilisateur	Gestion des autorisations			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
GetEventRule	Accorde l'autorisation d'obtenir un EventRule	Lecture	EventRule*		
GetFeatureOptInStatus [autorisation uniquement]	Accorde l'autorisation de lire le statut d'opt-in d'une fonctionnalité du service de notification AWS utilisateur	Lecture			
GetManagedNotificationChildEvent	Accorde l'autorisation d'obtenir une notification gérée pour les enfants	Lecture	ManagedNotificationChildEvent*		
GetManagedNotificationConfiguration	Accorde l'autorisation d'obtenir une configuration de notification gérée	Lecture	ManagedNotificationConfiguration*		
GetManagedNotificationEvent	Accorde l'autorisation d'obtenir un Managed NotificationEvent	Lecture	ManagedNotificationEvent*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetNotificationConfiguration	Donne l'autorisation d'obtenir un NotificationConfiguration	Lecture	NotificationConfiguration*		
GetNotificationEvent	Donne l'autorisation d'obtenir un NotificationEvent	Lecture	NotificationEvent*		
GetNotificationsAccessForOrganization	Accorde l'autorisation de lire Service Trust pour les notifications AWS utilisateur	Lecture			
ListChannels	Accorde l'autorisation de répertorier les chaînes par NotificationConfiguration	List	NotificationConfiguration*		
ListEventRules	Accorde l'autorisation de mettre en vente EventRules	List			
ListManagedNotificationChannelAssociations	Accorde l'autorisation de répertorier les contacts du compte et les canaux associés à une configuration de notification gérée	List	ManagedNotificationConfiguration*		
ListManagedNotificationChildEvents	Accorde l'autorisation de répertorier les événements Managed Notification Child	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListManagedNotificationConfigurations	Accorde l'autorisation de répertorier les configurations de notifications gérées	List			
ListManagedNotificationEvents	Accorde l'autorisation de répertorier les événements de notification gérés	List			
ListMemberAccounts	Accorde l'autorisation de répertorier les comptes membres pour une configuration de notification	List	NotificationConfiguration*		
ListNotificationConfigurations	Accorde l'autorisation de mettre en vente NotificationConfigurations	List			
ListNotificationEvents	Accorde l'autorisation de mettre en vente NotificationEvents	List			
ListNotificationHubs	Accorde l'autorisation de mettre en vente NotificationHubs	List			
ListOrganizationalUnits	Accorde l'autorisation de répertorier les unités organisationnelles pour une configuration de notification	List	NotificationConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Octroie l'autorisation d'obtenir les balises d'une ressource.	List			
PutFeatureOptInStatus [autorisation uniquement]	Accorde l'autorisation de mettre à jour le statut d'opt-in d'une fonctionnalité du service de notification AWS utilisateur	Écrire			
RegisterNotificationHub	Accorde l'autorisation d'enregistrer un NotificationHub	Écrire			
TagResource	Accorde l'autorisation de baliser une ressource	Identification	NotificationConfiguration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	NotificationConfiguration*		
				aws:TagKeys	
UpdateEventRule	Accorde l'autorisation de mettre à jour un EventRule	Écrire	EventRule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNotificationConfiguration	Accorde l'autorisation de mettre à jour un NotificationConfiguration	Écrire	NotificationConfiguration*		

Types de ressources définis par les notifications AWS utilisateur

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
EventRule	`arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}/rule/${EventRuleId}`	
NotificationConfiguration	`arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}`	aws:ResourceTag/${TagKey}
NotificationEvent	`arn:${Partition}:notifications:${Region}:${Account}:configuration/${NotificationConfigurationId}/event/${NotificationEventId}`	

Types de ressources	ARN	Clés de condition
ManagedNotificationChildEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}/child-event/${NotificationChildEventId}	
ManagedNotificationConfiguration	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}	
ManagedNotificationEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}	

Clés de condition pour les notifications aux AWS utilisateurs

AWS Les notifications utilisateur définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les contacts relatifs aux notifications AWS utilisateur

AWS User Notifications Contacts (préfixe de service :`notifications-contacts`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les contacts des notifications AWS utilisateur
- Types de ressources définis par AWS User Notifications Contacts
- Clés de condition pour les contacts AWS relatifs aux notifications utilisateur

Actions définies par les contacts des notifications AWS utilisateur

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ActivateEmailContact	Octroie l'autorisation d'activer le contact e-mail associé à l'ARN donné si le code fourni est valide.	Écrire	EmailContactResource*		
CreateEmailContact	Octroie l'autorisation de créer un contact e-mail.	Écrire		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteEmailContact	Octroie l'autorisation de supprimer un contact e-mail associé à l'ARN donné.	Écrire	EmailContactResource*		
GetEmailContact	Octroie l'autorisation d'obtenir un contact e-mail associé à l'ARN donné.	Lecture	EmailContactResource*		
ListEmailContacts	Octroie l'autorisation de répertorier les contacts e-mail.	List			
ListTagsForResource	Octroie l'autorisation d'obtenir les balises d'une ressource.	Lecture			
SendActivationCode	Octroie l'autorisation d'envoyer un lien d'activation à l'adresse	Écrire	EmailContactResource*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	e-mail associée à l'ARN donné.				
TagResource	Accorde l'autorisation de baliser une ressource	Identification	EmailContactResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer des identifications d'une ressource.	Identification	EmailContactResource*		
				aws:TagKeys	

Types de ressources définis par AWS User Notifications Contacts

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
EmailContactResource	`arn:${Partition}:notifications-contacts::${Account}:emailcontact/${EmailContactId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les contacts AWS relatifs aux notifications utilisateur

AWS User Notifications Contacts définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour les abonnements AWS utilisateur

AWS Les abonnements utilisateur (préfixe de service :`user-subscriptions`) fournissent les ressources, actions et clés contextuelles de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les abonnements des AWS utilisateurs
- Types de ressources définis par les abonnements des AWS utilisateurs
- Clés de condition pour les abonnements des AWS utilisateurs

Actions définies par les abonnements des AWS utilisateurs

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateClaim	Accorde l'autorisation de créer une réclamation d'abonnement utilisateur	Écrire		user-subscriptions:CreateForSelf	
DeleteClaim	Accorde l'autorisation de supprimer une réclamation d'abonnement utilisateur	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListApplicationClaims	Accorde l'autorisation de répertorier toutes les demandes d'abonnement des utilisateurs pour l'application	List			
ListClaims	Accorde l'autorisation de répertorier toutes les demandes d'abonnement des utilisateurs	List			
ListUserSubscriptions	Accorde l'autorisation de répertorier tous les abonnements des utilisateurs	List			
SetOverageConfig	Accorde l'autorisation de définir une configuration d'excédent d'abonnement utilisateur	Écrire			
UpdateClaim	Accorde l'autorisation de mettre à jour une demande d'abonnement utilisateur	Écrire			

Types de ressources définis par les abonnements des AWS utilisateurs

AWS User Subscriptions ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès aux abonnements AWS utilisateur, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour les abonnements des AWS utilisateurs

AWS Les abonnements utilisateur définissent les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
user-subscriptions:CreateForSelf	Filtre l'accès en autorisant uniquement la création de demandes d'abonnement utilisateur pour l'appelant	Booléen

Actions, ressources et clés de condition pour l'accès AWS vérifié

AWS Verified Access (préfixe de service :`verified-access`) fournit les ressources, actions et clés contextuelles de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Verified Access
- Types de ressources définis par AWS Verified Access
- Clés de condition pour l'accès AWS vérifié

Actions définies par AWS Verified Access

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVerifiedAccess [autorisation uniquement]	Accorde l'autorisation de créer une instance Verified Access	Écrire			

Types de ressources définis par AWS Verified Access

AWS Verified Access ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à AWS Verified Access, spécifiez `"Resource": "*"` dans votre politique.

Clés de condition pour l'accès AWS vérifié

Verified Access ne dispose pas de clés de contexte spécifiques aux services qui peuvent être utilisées dans l'élément `Condition` des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon Verified Permissions

Amazon Verified Permissions (préfixe de service : `verifiedpermissions`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon Verified Permissions
- Types de ressources définis par Amazon Verified Permissions
- Clés de condition pour Amazon Verified Permissions

Actions définies par Amazon Verified Permissions

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIdentitySource	Accorde l'autorisation de créer une référence à un fournisseur d'identité (IdP) externe compatible avec le protocole d'authentification OpenID Connect (OIDC), tel qu'Amazon Cognito	Écrire	policy-store*		
CreatePolicy	Accorde l'autorisation de créer une politique Cedar et de	Écrire	policy-store*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	l'enregistrer dans le magasin de politiques spécifié				
CreatePolicyStore	Accorde l'autorisation de créer une politique Cedar et de l'enregistrer dans le magasin de politiques spécifié	Écrire		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyTemplate	Accorde l'autorisation de créer un modèle de politique	Écrire	policy-store*		
DeleteIdentitySource	Accorde l'autorisation de supprimer une source d'identité qui fait référence à un fournisseur d'identité (IdP), tel qu'Amazon Cognito	Écrire	policy-store*		
DeletePolicy	Accorde l'autorisation de supprimer la politique spécifiée du magasin de politiques	Écrire	policy-store*		
DeletePolicyStore	Accorde l'autorisation de supprimer le magasin de politiques spécifié	Écrire	policy-store*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeletePolicyTemplate	Accorde l'autorisation de supprimer le modèle de politique spécifié du magasin de politiques	Écrire	policy-store*		
GetIdentitySource	Accorde l'autorisation de récupérer des informations sur la source d'identité spécifiée	Lecture	policy-store*		
GetPolicy	Accorde l'autorisation de récupérer des informations sur la politique spécifiée	Lecture	policy-store*		
GetPolicyStore	Accorde l'autorisation de récupérer des informations sur un magasin de politiques	Lecture	policy-store*		verifiedpermissions:ListTagsForResource
GetPolicyTemplate	Accorde l'autorisation de récupérer les informations du modèle de politique spécifié dans le magasin de politiques spécifié	Lecture	policy-store*		
GetSchema	Accorde l'autorisation de récupérer les informations du schéma spécifié dans le magasin de politiques spécifié	Lecture	policy-store*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
IsAuthorized	Accorde l'autorisation de prendre une décision d'autorisation quant à une demande de service décrite dans les paramètres	Lecture	policy-store*		
IsAuthorizedWithToken	Accorde l'autorisation de prendre une décision d'autorisation quant à une demande de service décrite dans les paramètres. Le principal de cette demande provient d'une source d'identité externe	Lecture	policy-store*		
ListIdentitySources	Accorde l'autorisation de renvoyer une liste paginée de toutes les sources d'identité définies dans le magasin de politiques spécifié	List	policy-store*		
ListPolicies	Accorde l'autorisation de renvoyer une liste paginée de toutes les politiques stockées dans le magasin de politiques spécifié	List	policy-store*		
ListPolicyStores	Accorde l'autorisation de renvoyer une liste paginée de tous les magasins de politiques dans le compte Amazon Web Services appelant	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListPolicyTemplates	Accorde l'autorisation de renvoyer une liste paginée de tous les modèles de politique dans le magasin de politiques spécifié	List	policy-store*		
ListTagsForResource	Accorde l'autorisation d'afficher une liste de balises de ressources pour le magasin de politiques spécifié	Lecture	policy-store*		
PutSchema	Accorde l'autorisation de créer ou de mettre à jour un schéma de politique dans le magasin de politiques spécifié	Écrire	policy-store*		
TagResource	Accorde l'autorisation d'ajouter des balises au magasin de politiques spécifié	Identification	policy-store*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer des balises du magasin de politiques spécifié	Identification	policy-store*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateIdentitySource	Accorde l'autorisation de mettre à jour la source d'identité spécifiée afin d'utiliser une nouvelle source de fournisseur d'identité (IdP) ou de modifier le mappage des identités de l'IdP vers un autre type d'entité principale	Écrire	policy-store*		
UpdatePolicy	Accorde l'autorisation de modifier la politique statique Cedar spécifiée dans le magasin de politiques spécifié	Écrire	policy-store*		
UpdatePolicyStore	Accorde l'autorisation de modifier les paramètres de validation d'un magasin de politiques	Écrire	policy-store*		
UpdatePolicyTemplate	Accorde l'autorisation de mettre à jour le modèle de politique spécifié	Écrire	policy-store*		

Types de ressources définis par Amazon Verified Permissions

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
policy-store	`arn:${Partition}:verifiedpermissions::${Account}:policy-store/${PolicyStoreId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon Verified Permissions

Amazon Verified Permissions définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la paire de clés et de valeurs d'identification autorisée dans la demande.	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la paire de clé et de valeur d'identification d'une ressource.	Chaîne
aws:TagKeys	Filtre l'accès en fonction d'une liste de clés d'identification autorisées dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour Amazon VPC Lattice

Amazon VPC Lattice (préfixe de service : `vpc-lattice`) fournissent les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon VPC Lattice
- Types de ressources définis par Amazon VPC Lattice
- Clés de condition pour Amazon VPC Lattice

Actions définies par Amazon VPC Lattice

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateViaAWSService [autorisation uniquement]	Accorde l'autorisation d'associer une configuration de ressources via n'importe quel réseau géré par des AWS services	Gestion des autorisations			
AssociateViaAWSService-EventsAndStates	Accorde l'autorisation d'associer une configuration de ressources via les réseaux de services Amazon EventBridge et AWS Step Functions	Gestion des autorisations			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
CreateAccessLogSubscription	Accorde l'autorisation de créer un abonnement aux journaux d'accès	Écrire	AccessLogSubscription*		logs:CreateLogDelivery logs:GetLogDelivery
			ResourceConfiguration		
			Service		
			ServiceNetwork		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction	
CreateListener	Accorde l'autorisation de créer un écouteur	Écrire	Listener*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns vpc-lattice:CreateAction	
CreateResourceConfiguration	Accorde l'autorisation de créer une configuration de ressources	Écrire	DomainVerification		
			ResourceConfiguration		
			ResourceGateway		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction	
CreateResourceGateway	Accorde l'autorisation de créer une passerelle de ressources	Écrire	ResourceGateway*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId vpc-lattice:CreateAction	
CreateRule	Accorde l'autorisation de créer une règle	Écrire	Rule*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns vpc-lattice:CreateAction	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateService	Accorde l'autorisation de créer un service	Écrire	Service*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction	
CreateServiceNetwork	Accorde l'autorisation de créer un réseau de services	Écrire	ServiceNetwork*		iam:CreateServiceLinkedRole

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction	
CreateServiceNetworkResourceAssociation	Accorde l'autorisation de créer une association entre un réseau de services et une ressource	Écrire	ResourceConfiguration*		
			ServiceNetwork*		
			ServiceNetworkResourceAssociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn vpc-lattice:CreateAction	
CreateServiceNetworkServiceAssociation	Accorde l'autorisation de créer un réseau de services et une association de services	Écrire	Service*		
			ServiceNetwork*		
			ServiceNetworkServiceAssociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn vpc-lattice:CreateAction	
CreateServiceNetworkVpcAssociation	Accorde l'autorisation de créer un réseau de services et une association de VPC	Écrire	ServiceNetwork* ServiceNetworkVpcAssociation*		ec2:DescribeVpcs

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:PrivateDnsPreference vpc-lattice:PrivateDnsSpecifiedDomains vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				vpc-lattice:CreateAction	
CreateServiceNetworkVpcEndpointAssociation [autorisation uniquement]	Accorde l'autorisation de créer une association entre un réseau de services et un point de terminaison VPC	Gestion des autorisations			
CreateTargetGroup	Accorde l'autorisation de créer un groupe cible	Écrire	TargetGroup*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId vpc-lattice:CreateAction	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAccessLogSubscription	Accorde l'autorisation de supprimer un abonnement aux journaux d'accès	Écrire	AccessLogSubscription*		logs:DeleteLogDelivery logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
DeleteAuthPolicy	Accorde l'autorisation de supprimer une politique d'authentification	Gestion des autorisations	Service		
			ServiceNetwork		
DeleteDomainVerification	Accorde l'autorisation de supprimer une vérification de domaine	Écrire	DomainVerification*		
				aws:ResourceTag/${TagKey}	
DeleteListener	Accorde l'autorisation de supprimer un écouteur	Écrire	Listener*		
				aws:ResourceTag/${TagKey}	
DeleteResourceConfiguration	Accorde l'autorisation de supprimer une configuration de ressource	Écrire	ResourceConfiguration*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteResourceEndpointAssociation	Accorde l'autorisation de supprimer une association de point de terminaison de ressource	Écrire	ResourceEndpointAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteResourceGateway	Autorise la suppression d'une passerelle de ressources	Écrire	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Accorde l'autorisation de supprimer une politique de ressource	Écrire	ResourceConfiguration		
			Service		
			ServiceNetwork		
DeleteRule	Accorde l'autorisation de supprimer une règle	Écrire	Rule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteService	Accorde l'autorisation de supprimer un service	Écrire	Service*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetwork	Accorde l'autorisation de supprimer un réseau de services	Écrire	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkResourceAssociation	Accorde l'autorisation de supprimer l'association entre un réseau de service et une ressource	Écrire	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkServiceAssociation	Accorde l'autorisation de supprimer une association de services de réseau de services	Écrire	ServiceNetworkServiceAssociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
DeleteServiceNetworkVpcAssociation	Accorde l'autorisation de supprimer un réseau de services et une association de VPC	Écrire	ServiceNetworkVpcAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
DeleteTargetGroup	Accorde l'autorisation de supprimer un groupe cible	Écrire	TargetGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeregisterTargets	Accorde l'autorisation d'annuler l'enregistrement des cibles d'un groupe cible	Écrire	TargetGroup*		
GetAccessLogSubscription	Accorde l'autorisation d'obtenir des informations sur un abonnement de journaux d'accès	Lecture	AccessLogSubscription*		logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
GetAuthPolicy	Accorde l'autorisation d'obtenir des informations sur une politique d'authentification	Lecture	Service		
			ServiceNetwork		
GetDomainVerification	Accorde l'autorisation d'obtenir des informations sur la vérification d'un domaine	Lecture	DomainVerification*		
				aws:ResourceTag/${TagKey}	
GetListener	Accorde l'autorisation d'obtenir des informations sur un écouteur	Lecture	Listener*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetResourceConfiguration	Accorde l'autorisation d'obtenir des informations sur la configuration d'une ressource	Lecture	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
GetResourceGateway	Accorde l'autorisation d'obtenir des informations sur une passerelle de ressources	Lecture	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Accorde l'autorisation d'obtenir des informations sur une politique de ressources	Lecture	ResourceConfiguration		
			Service		
			ServiceNetwork		
GetRule	Accorde l'autorisation d'obtenir des informations sur une règle	Lecture	Rule*		
				aws:ResourceTag/${TagKey}	
GetService	Accorde l'autorisation d'obtenir des informations sur un service	Lecture	Service*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetServiceNetwork	Accorde l'autorisation d'obtenir des informations sur un réseau de services	Lecture	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
GetServiceNetworkResourceAssociation	Accorde l'autorisation d'obtenir des informations sur une association entre un réseau de services et la configuration des ressources	Lecture	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
GetServiceNetworkServiceAssociation	Accorde l'autorisation d'obtenir des informations sur un réseau de services et une association de services	Lecture	ServiceNetworkServiceAssociation*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
GetServiceNetworkVpcAssociation	Accorde l'autorisation d'obtenir des informations sur un réseau de services et une association de VPC	Lecture	ServiceNetworkVpcAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
GetTargetGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de cible	Lecture	TargetGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ListAccessLogSubscriptions	Accorde l'autorisation de répertorier une partie ou la totalité des abonnements aux journaux d'accès concernant un réseau de services ou un service	List			
ListDomainVerifications	Accorde l'autorisation de répertorier certaines ou toutes les vérifications de domaine	List			
ListListeners	Accorde l'autorisation de répertorier une partie ou la totalité des écouteurs	List			
ListResourceConfigurations	Accorde l'autorisation de répertorier certaines ou toutes les configurations de ressources	List			
ListResourceEndpointAssociations	Accorde l'autorisation de répertorier certaines ou toutes les associations entre une configuration de ressources et un point de terminaison VPC	List		vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourceGateways	Accorde l'autorisation de répertorier certaines ou toutes les passerelles de ressources	List			
ListRules	Accorde l'autorisation de répertorier une partie ou la totalité des règles	List			
ListServiceNetworkResourceAssociations	Accorde l'autorisation de répertorier certaines ou toutes les associations entre un réseau de services et la configuration des ressources	List			
ListServiceNetworkServiceAssociations	Accorde l'autorisation de répertorier une partie ou la totalité des réseaux de services et associations de services	List		vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
ListServiceNetworkVpcAssociations	Accorde l'autorisation de répertorier une partie ou la totalité des réseaux de services et associations de VPC	List		vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListServiceNetworkVpcEndpointAssociations	Accorde l'autorisation de répertorier certaines ou toutes les associations entre un réseau de services et un point de terminaison VPC	List			
ListServiceNetworks	Accorde l'autorisation de répertorier les réseaux de services appartenant à un compte d'appelant ou partagés avec celui-ci	List			
ListServices	Accorde l'autorisation de répertorier les services appartenant à un compte d'appelant ou partagés avec celui-ci	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource vpc-lattice	Lecture			
ListTargetGroups	Accorde l'autorisation de répertorier une partie ou la totalité des groupes cibles	List			
ListTargets	Accorde l'autorisation de répertorier une partie ou la totalité des cibles dans un groupe cible	List	TargetGroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutAuthPolicy	Accorde l'autorisation de créer ou de mettre à jour la politique d'authentification pour un réseau de services ou un service	Gestion des autorisations	Service		
			ServiceNetwork		
PutResourcePolicy	Accorde l'autorisation de créer une politique de ressources pour une configuration de ressources, un service ou un réseau de services	Écrire	ResourceConfiguration		
			Service		
			ServiceNetwork		
RegisterTargets	Accorde l'autorisation d'enregistrer des cibles à un groupe cible	Écrire	TargetGroup*		
StartDomainVerification	Accorde l'autorisation de démarrer une vérification de domaine	Écrire	DomainVerification*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:DomainName vpc-lattice:CreateAction	
TagResource	Accorde l'autorisation de baliser une ressource vpc-lattice	Identification	AccessLogSubscription		
			DomainVerification		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource vpc-lattice	Identification	AccessLogSubscription		
			DomainVerification		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		
			ResourceGateway		
			Rule		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			Service		
			ServiceNetwork		
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		
				aws:TagKeys	
UpdateAccessLogSubscription	Accorde l'autorisation de mettre à jour un abonnement aux journaux d'accès	Écrire	AccessLogSubscription*		logs:GetLogDelivery logs:UpdateLogDelivery

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateListener	Accorde l'autorisation de mettre à jour un écouteur	Écrire	Listener*		
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateResourceConfiguration	Accorde l'autorisation de mettre à jour une configuration de ressource	Écrire	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateResourceGateway	Autorise la mise à jour d'une passerelle de ressources	Écrire	ResourceGateway*		
				aws:ResourceTag/${TagKey} vpc-lattice:SecurityGroupIds	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRule	Accorde l'autorisation de mettre à jour une règle	Écrire	Rule*		
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateService	Accorde l'autorisation de mettre à jour un service	Écrire	Service*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	
UpdateServiceNetwork	Accorde l'autorisation de mettre à jour un réseau de service	Écrire	ServiceNetwork*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateServiceNetworkVpcAssociation	Accorde l'autorisation de mettre à jour un réseau de services et une association de VPC	Écrire	ServiceNetworkVpcAssociation*		ec2:DescribeSecurityGroups ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
UpdateTargetGroup	Accorde l'autorisation de mettre à jour un groupe cible	Écrire	TargetGroup*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon VPC Lattice

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
AccessLog Subscription	`arn:${Partition}:vpc-lattice:${Region}:${Account}:accesslogsubscription/${AccessLogSubscriptionId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction
DomainVerification	`arn:${Partition}:vpc-lattice:${Region}:${Account}:domainverification/${DomainVerificationId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:DomainName
Listener	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}`	aws:RequestTag/${TagKey}

Types de ressources	ARN	Clés de condition
		aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:Protocol vpc-lattice:TargetGroupArns
ResourceConfiguration	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceconfiguration/${ResourceConfigurationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction
ResourceEndpointAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceendpointassociation/${ResourceEndpointAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId

Types de ressources	ARN	Clés de condition
ResourceGateway	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourcegateway/${ResourceGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:VpcId
Rule	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}/rule/${RuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:TargetGroupArns

Types de ressources	ARN	Clés de condition
Service	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction
ServiceNetwork	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetwork/${ServiceNetworkId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction

Types de ressources	ARN	Clés de condition
ServiceNetworkResourceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkresourceassociation/${ServiceNetworkResourceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn
ServiceNetworkServiceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkserviceassociation/${ServiceNetworkServiceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn

Types de ressources	ARN	Clés de condition
ServiceNetworkVpcAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkvpcassociation/${ServiceNetworkVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:PrivateDnsPreference vpc-lattice:PrivateDnsSpecifiedDomains vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId

Types de ressources	ARN	Clés de condition
TargetGroup	`arn:${Partition}:vpc-lattice:${Region}:${Account}:targetgroup/${TargetGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:VpcId

Clés de condition pour Amazon VPC Lattice

Amazon VPC Lattice définissent les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la présence de paires clé-valeur d'identification dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Clés de condition	Description	Type
vpc-lattice:AuthType	Filtre l'accès en fonction du type d'authentification spécifié dans la demande	String
vpc-lattice:CreateAction	Filtre l'accès en fonction du nom d'une action d'API de création de ressources.	String
vpc-lattice:DomainName	Filtre l'accès par nom de domaine	String
vpc-lattice:PrivateDnsPreference	Filtre l'accès en fonction de la préférence DNS privée	String
vpc-lattice:PrivateDnsSpecifiedDomains	Filtre l'accès par les domaines DNS privés	ArrayOfString
vpc-lattice:Protocol	Filtre l'accès en fonction du protocole spécifié dans la demande	String
vpc-lattice:ResourceConfigurationArn	Filtre l'accès par l'ARN d'une configuration de ressource	ARN
vpc-lattice:SecurityGroupIds	Filtre l'accès en fonction IDs des groupes de sécurité	ArrayOfString
vpc-lattice:ServiceArn	Filtre l'accès en fonction de l'ARN d'un service	ARN
vpc-lattice:ServiceNetworkArn	Filtre l'accès en fonction de l'ARN d'un réseau de services	ARN

Clés de condition	Description	Type
vpc-lattice:TargetGroupArns	Filtre l'accès par groupes cibles ARNs	ArrayOfARN
vpc-lattice:VpcEndpointId	Filtre l'accès en fonction de l'ID d'un point de terminaison VPC	String
vpc-lattice:VpcId	Filtre l'accès par l'ID d'un cloud privé virtuel (VPC).	String

Actions, ressources et clés de condition pour les services Amazon VPC Lattice

Les services Amazon VPC Lattice (préfixe de service : `vpc-lattice-svcs`) fournissent les ressources, les actions et les clés de contexte de condition spécifiques au service suivantes en vue de leur utilisation dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les services Amazon VPC Lattice
- Types de ressources définis par les services Amazon VPC Lattice
- Clés de condition pour les services Amazon VPC Lattice

Actions définies par les services Amazon VPC Lattice

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Connect	Accorde l'autorisation de se connecter à un service VPC Lattice	Écrire	TCP Service*		
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount	
Invoke	Accorde l'autorisation pour invoquer un service VPC Lattice	Écrire	Service*		
				vpc-lattice-svcs:Port	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount vpc-lattice-svcs:RequestMethod vpc-lattice-svcs:RequestPath vpc-lattice-	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				svcs:RequestHeader/${HeaderName} vpc-lattice-svcs:RequestQueryString/${QueryStringKey}	

Types de ressources définis par les services Amazon VPC Lattice

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/${RequestPath}`	

Types de ressources	ARN	Clés de condition
TCP Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}`	

Clés de condition pour les services Amazon VPC Lattice

Les services Amazon VPC Lattice définissent les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
vpc-lattice-svcs:Port	Filtre l'accès en fonction du port de destination auquel la demande est adressée	Numérique
vpc-lattice-svcs:RequestHeader/${HeaderName}	Filtre l'accès en fonction d'une paire nom-valeur dans les en-têtes de la demande	String
vpc-lattice-svcs:RequestMethod	Filtre l'accès en fonction de la méthode de la requête	String
vpc-lattice-svcs:RequestPath	Filtre l'accès en fonction de la partie chemin de l'URL de demande	String
vpc-lattice-svcs:RequestQueryString/	Filtre l'accès en fonction des paires clé-valeur de la chaîne de requête dans l'URL de la demande	ArrayOfString

Clés de condition	Description	Type
${QueryStringKey}		
vpc-lattice-svcs:ServiceArn	Filtre l'accès en fonction de l'ARN du service recevant la requête	ARN
vpc-lattice-svcs:ServiceNetworkArn	Filtre l'accès en fonction de l'ARN du réseau de service recevant la requête	ARN
vpc-lattice-svcs:SourceVpc	Filtre l'accès en fonction du VPC d'où provient la requête	String
vpc-lattice-svcs:SourceVpcOwnerAccount	Filtre l'accès en fonction du compte propriétaire du VPC d'où provient la requête	String

Actions, ressources et clés de condition pour AWS WAF

AWS Le WAF (préfixe de service :`waf`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par le AWS WAF
- Types de ressources définis par AWS WAF
- Clés de condition pour AWS WAF

Actions définies par le AWS WAF

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateByteMatchSet	Accorde l'autorisation de créer un ByteMatchSet	Écrire	bytematchset*		
CreateGeoMatchSet	Accorde l'autorisation de créer un GeoMatchSet	Écrire	geomatchset*		
CreateIPSet	Accorde l'autorisation de créer un IPSet	Écrire	ipset*		
CreateRateBasedRule	Accorde l'autorisation de créer un RateBasedRule pour limiter le volume de demandes provenant d'une seule adresse IP	Écrire	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Accorde l'autorisation de créer un RegexMatchSet	Écrire	regexmatchset*		
CreateRegexPatternSet	Accorde l'autorisation de créer un RegexPatternSet	Écrire	regexpatternset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateRule	Accorde l'autorisation de créer une règle pour filtrer les demandes web	Écrire	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Accorde l'autorisation de créer un RuleGroup ensemble de règles prédéfinies que vous pouvez utiliser dans un WebACL	Écrire	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Accorde l'autorisation de créer un SizeConstraintSet	Écrire	sizeconstraintset*		
CreateSqlInjectionMatchSet	Accorde l'autorisation de créer un SqlInjectionMatchSet	Écrire	sqlinjectionmatchset*		
CreateWebACL	Accorde l'autorisation de créer un élément WebACL qui contient des règles de filtrage des requêtes web	Gestion des autorisations	webacl*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Accorde l'autorisation de créer un modèle d'ACL CloudFormation Web dans un compartiment S3 dans le but de migrer l'ACL Web de AWS WAF Classic vers AWS WAF v2	Écrire	webacl*		s3:PutObject
CreateXssMatchSet	Accorde l'autorisation de créer un XssMatchSet, que vous utilisez pour détecter les demandes contenant des attaques par script intersite	Écrire	xssmatchset*		
DeleteByteMatchSet	Accorde l'autorisation de supprimer un ByteMatchSet	Écrire	bytematchset*		
DeleteGeoMatchSet	Accorde l'autorisation de supprimer un GeoMatchSet	Écrire	geomatchset*		
DeleteIPSet	Accorde l'autorisation de supprimer un IPSet	Écrire	ipset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLoggingConfiguration	Accorde l'autorisation de supprimer le LoggingConfiguration depuis une ACL Web	Écrire	webacl*		
DeletePermissionPolicy	Accorde l'autorisation de supprimer une politique IAM d'un groupe de règles	Gestion des autorisations	rulegroup*		
DeleteRateBasedRule	Accorde l'autorisation de supprimer un RateBasedRule	Écrire	ratebasedrule*		
DeleteRegexMatchSet	Accorde l'autorisation de supprimer un RegexMatchSet	Écrire	regexmatchset*		
DeleteRegexPatternSet	Accorde l'autorisation de supprimer un RegexPatternSet	Écrire	regexpatternset*		
DeleteRule	Accorde l'autorisation de supprimer un élément Rule	Écrire	rule*		
DeleteRuleGroup	Accorde l'autorisation de supprimer un RuleGroup	Écrire	rulegroup*		
DeleteSizeConstraintSet	Accorde l'autorisation de supprimer un SizeConstraintSet	Écrire	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Accorde l'autorisation de supprimer un SqlInjectionMatchSet	Écrire	sqlinjectionmatchset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteWebACL	Accorde l'autorisation de supprimer un élément WebACL	Gestion des autorisations	webacl*		
DeleteXssMatchSet	Accorde l'autorisation de supprimer un XssMatchSet	Écrire	xssmatchset*		
GetByteMatchSet	Accorde l'autorisation de récupérer un ByteMatchSet	Lecture	bytematchset*		
GetChangeToken	Accorde l'autorisation de récupérer un jeton de modification à utiliser dans les demandes de création, de mise à jour et de suppression	Lecture			
GetChangeTokenStatus	Accorde l'autorisation de récupérer l'état d'un jeton de modification	Lecture			
GetGeoMatchSet	Accorde l'autorisation de récupérer un GeoMatchSet	Lecture	geomatchset*		
GetIPSet	Accorde l'autorisation de récupérer un IPSet	Lecture	ipset*		
GetLoggingConfiguration	Accorde l'autorisation de récupérer une ACL LoggingConfiguration pour un site Web	Lecture	webacl*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPermissionPolicy	Accorde l'autorisation de récupérer une politique IAM pour un groupe de règles	Lecture	rulegroup*		
GetRateBasedRule	Accorde l'autorisation de récupérer un RateBasedRule	Lecture	ratebasedrule*		
GetRateBasedRuleManagedKeys	Accorde l'autorisation de récupérer le tableau d'adresses IP actuellement bloquées par un RateBasedRule	Lecture	ratebasedrule*		
GetRegexMatchSet	Accorde l'autorisation de récupérer un RegexMatchSet	Lecture	regexmatchset*		
GetRegexPatternSet	Accorde l'autorisation de récupérer un RegexPatternSet	Lecture	regexpatternset*		
GetRule	Accorde l'autorisation de récupérer un élément Rule	Lecture	rule*		
GetRuleGroup	Accorde l'autorisation de récupérer un RuleGroup	Lecture	rulegroup*		
GetSampledRequests	Accorde l'autorisation de récupérer des informations détaillées sur un jeu d'échantillons de requêtes web	Lecture	webacl		
GetSizeConstraintSet	Accorde l'autorisation de récupérer un SizeConstraintSet	Lecture	sizeconstraintset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSqlInjectionMatchSet	Accorde l'autorisation de récupérer un SqlInjectionMatchSet	Lecture	sqlinjectionmatchset*		
GetWebACL	Accorde l'autorisation de récupérer un élément WebACL	Lecture	webacl*		
GetXssMatchSet	Accorde l'autorisation de récupérer un XssMatchSet	Lecture	xssmatchset*		
ListActivatedRulesInRuleGroup	Accorde l'autorisation de récupérer un tableau d'ActivatedRule objets	List			
ListByteMatchSets	Accorde l'autorisation de récupérer un tableau d'ByteMatchSetSummary objets	List			
ListGeoMatchSets	Accorde l'autorisation de récupérer un tableau d'GeoMatchSetSummary objets	List			
ListIPSets	Accorde l'autorisation de récupérer un tableau d'objets IPSet Summary	List			
ListLoggingConfigurations	Accorde l'autorisation de récupérer un tableau d'LoggingConfiguration objets	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRateBasedRules	Accorde l'autorisation de récupérer un tableau d' RuleSummary objets	List			
ListRegexMatchSets	Accorde l'autorisation de récupérer un tableau d' RegexMatchSetSummary objets	List			
ListRegexPatternSets	Accorde l'autorisation de récupérer un tableau d' RegexPatternSetSummary objets	List			
ListRuleGroups	Accorde l'autorisation de récupérer un tableau d' RuleGroup objets	List			
ListRules	Accorde l'autorisation de récupérer un tableau d' RuleSummary objets	List			
ListSizeConstraintSets	Accorde l'autorisation de récupérer un tableau d' SizeConstraintSetSummary objets	List			
ListSqlInjectionMatchSets	Accorde l'autorisation de récupérer un tableau d' SqlInjectionMatchSet objets	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListSubscribedRuleGroups	Accorde l'autorisation de récupérer un tableau d'RuleGroup objets auxquels vous êtes abonné	List			
ListTagsForResource	Accorde l'autorisation de récupérer les balises d'une ressource	Lecture	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Accorde l'autorisation de récupérer un tableau d'ACLSummary objets Web	List			
ListXssMatchSets	Accorde l'autorisation de récupérer un tableau d'XssMatchSet objets	List			
PutLoggingConfiguration	Accorde l'autorisation d'LoggingConfiguration associer un à une ACL Web spécifiée	Écrire	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	Accorde l'autorisation d'attacher une politique IAM à un groupe de règles, de partager le groupe de règles entre des comptes	Gestion des autorisations	rulegroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource	Balisage	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	Accorde l'autorisation d'insérer ou de supprimer ByteMatch Tuple des objets dans un ByteMatchSet	Écrire	bytematchset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGeoMatchSet	Accorde l'autorisation d'insérer ou de supprimer GeoMatchConstraint des objets dans un GeoMatchSet	Écrire	geomatchset*		
UpdateIPSet	Accorde l'autorisation d'insérer ou de supprimer des objets IPSet Descriptor dans un IPSet	Écrire	ipset*		
UpdateRateBasedRule	Accorde l'autorisation de modifier une règle basée sur les tarifs	Écrire	ratebasedrule*		
UpdateRegexMatchSet	Accorde l'autorisation d'insérer ou de supprimer RegexMatchTuple des objets dans un RegexMatchSet	Écrire	regexmatchset*		
UpdateRegexPatternSet	Accorde l'autorisation d'insérer ou de supprimer RegexPatternStrings dans un RegexPatternSet	Écrire	regexpatternset*		
UpdateRule	Accorde l'autorisation de modifier un élément Rule	Écrire	rule*		
UpdateRuleGroup	Accorde l'autorisation d'insérer ou de supprimer ActivatedRule des objets dans un RuleGroup	Écrire	rulegroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateSizeConstraintSet	Accorde l'autorisation d'insérer ou de supprimer SizeConstraint des objets dans un SizeConstraintSet	Écrire	sizeconstraintset*		
UpdateSqlInjectionMatchSet	Accorde l'autorisation d'insérer ou de supprimer SqlInjectionMatchTuple des objets dans un SqlInjectionMatchSet	Écrire	sqlinjectionmatchset*		
UpdateWebACL	Accorde l'autorisation d'insérer ou de supprimer ActivatedRule des objets dans un WebACL	Gestion des autorisations	webacl*		
UpdateXssMatchSet	Accorde l'autorisation d'insérer ou de supprimer XssMatchTuple des objets dans un XssMatchSet	Écrire	xssmatchset*		

Types de ressources définis par AWS WAF

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
bytematchset	arn:${Partition}:waf::${Account}:bytematchset/${Id}	
ipset	arn:${Partition}:waf::${Account}:ipset/${Id}	
ratebasedrule	arn:${Partition}:waf::${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf::${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf::${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf::${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf::${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf::${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf::${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf::${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf::${Account}:geomatchset/${Id}	
rulegroup	arn:${Partition}:waf::${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS WAF

AWS WAF définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de l'ensemble des valeurs autorisées pour chacune des balises.	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur de balise associée à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS WAF Regional

AWS WAF Regional (préfixe de service :`waf-regional`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS WAF Regional

- Types de ressources définis par AWS WAF Regional
- Clés de condition pour AWS WAF Regional

Actions définies par AWS WAF Regional

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateWebACL	Accorde l'autorisation d'associer une liste ACL web à une ressource	Écrire	loadbalancer/app/*		
			webacl*		
CreateByteMatchSet	Accorde l'autorisation de créer un ByteMatchSet	Écrire	bytematchset*		
CreateGeoMatchSet	Accorde l'autorisation de créer un GeoMatchSet	Écrire	geomatchset*		
CreateIPSet	Accorde l'autorisation de créer un IPSet	Écrire	ipset*		
CreateRateBasedRule	Accorde l'autorisation de créer un RateBasedRule	Écrire	ratebasedrule*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateRegexMatchSet	Accorde l'autorisation de créer un RegexMatchSet	Écrire	regexmatchset*		
CreateRegexPatternSet	Accorde l'autorisation de créer un RegexPatternSet	Écrire	regexpatternset*		
CreateRule	Accorde l'autorisation de créer un élément Rule	Écrire	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Accorde l'autorisation de créer un RuleGroup	Écrire	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Accorde l'autorisation de créer un SizeConstraintSet	Écrire	sizeconstraintset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateSqlInjectionMatchSet	Accorde l'autorisation de créer un SqlInjectionMatchSet	Écrire	sqlinjectionmatchset*		
CreateWebACL	Accorde l'autorisation de créer un élément WebACL	Gestion des autorisations	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Accorde l'autorisation de créer un modèle d'ACL CloudFormation Web dans un compartiment S3 dans le but de migrer l'ACL Web de AWS WAF Classic vers AWS WAF v2	Écrire	webacl*		s3:PutObject
CreateXssMatchSet	Accorde l'autorisation de créer un XssMatchSet	Écrire	xssmatchset*		
DeleteByteMatchSet	Accorde l'autorisation de supprimer un ByteMatchSet	Écrire	bytematchset*		
DeleteGeoMatchSet	Accorde l'autorisation de supprimer un GeoMatchSet	Écrire	geomatchset*		
DeleteIPSet	Accorde l'autorisation de supprimer un IPSet	Écrire	ipset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteLoggingConfiguration	Accorde l'autorisation de supprimer un LoggingConfiguration d'une ACL Web	Écrire	webacl*		
DeletePermissionPolicy	Accorde l'autorisation de supprimer une politique IAM d'un groupe de règles	Gestion des autorisations	rulegroup*		
DeleteRateBasedRule	Accorde l'autorisation de supprimer un RateBasedRule	Écrire	ratebasedrule*		
DeleteRegexMatchSet	Accorde l'autorisation de supprimer un RegexMatchSet	Écrire	regexmatchset*		
DeleteRegexPatternSet	Accorde l'autorisation de supprimer un RegexPatternSet	Écrire	regexpatternset*		
DeleteRule	Accorde l'autorisation de supprimer un élément Rule	Écrire	rule*		
DeleteRuleGroup	Accorde l'autorisation de supprimer un RuleGroup	Écrire	rulegroup*		
DeleteSizeConstraintSet	Accorde l'autorisation de supprimer un SizeConstraintSet	Écrire	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Accorde l'autorisation de supprimer un SqlInjectionMatchSet	Écrire	sqlinjectionmatchset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteWebACL	Accorde l'autorisation de supprimer un élément WebACL	Gestion des autorisations	webacl*		
DeleteXssMatchSet	Accorde l'autorisation de supprimer un XssMatchSet	Écrire	xssmatchset*		
DisassociateWebACL	Accorde l'autorisation de supprimer une association entre une liste ACL web et une ressource	Écrire	loadbalancer/app/*		
GetByteMatchSet	Accorde l'autorisation de récupérer un ByteMatchSet	Lecture	bytematchset*		
GetChangeToken	Accorde l'autorisation de récupérer un jeton de modification à utiliser dans les demandes de création, de mise à jour et de suppression	Lecture			
GetChangeTokenStatus	Accorde l'autorisation de récupérer l'état d'un jeton de modification	Lecture			
GetGeoMatchSet	Accorde l'autorisation de récupérer un GeoMatchSet	Lecture	geomatchset*		
GetIPSet	Accorde l'autorisation de récupérer un IPSet	Lecture	ipset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetLoggingConfiguration	Accorde l'autorisation de récupérer un LoggingConfiguration	Lecture	webacl*		
GetPermissionPolicy	Accorde l'autorisation de récupérer une politique IAM attachée à un RuleGroup	Lecture	rulegroup*		
GetRateBasedRule	Accorde l'autorisation de récupérer un RateBasedRule	Lecture	ratebasedrule*		
GetRateBasedRuleManagedKeys	Accorde l'autorisation de récupérer le tableau d'adresses IP actuellement bloquées par un RateBasedRule	Lecture	ratebasedrule*		
GetRegexMatchSet	Accorde l'autorisation de récupérer un RegexMatchSet	Lecture	regexmatchset*		
GetRegexPatternSet	Accorde l'autorisation de récupérer un RegexPatternSet	Lecture	regexpatternset*		
GetRule	Accorde l'autorisation de récupérer un élément Rule	Lecture	rule*		
GetRuleGroup	Accorde l'autorisation de récupérer un RuleGroup	Lecture	rulegroup*		
GetSampledRequests	Accorde l'autorisation de récupérer des informations détaillées pour un ensemble de demandes web	Lecture	webacl		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSizeConstraintSet	Accorde l'autorisation de récupérer un SizeConstraintSet	Lecture	sizeconstraintset*		
GetSqlInjectionMatchSet	Accorde l'autorisation de récupérer un SqlInjectionMatchSet	Lecture	sqlinjectionmatchset*		
GetWebACL	Accorde l'autorisation de récupérer un élément WebACL	Lecture	webacl*		
GetWebACLForResource	Accorde l'autorisation de récupérer un élément WebACL associé à une ressource spécifiée	Lecture	loadbalancer/app/*		
GetXssMatchSet	Accorde l'autorisation de récupérer un XssMatchSet	Lecture	xssmatchset*		
ListActivatedRulesInRuleGroup	Accorde l'autorisation de récupérer un tableau d'ActivatedRule objets	List			
ListByteMatchSets	Accorde l'autorisation de récupérer un tableau d'ByteMatchSetSummary objets	List			
ListGeoMatchSets	Accorde l'autorisation de récupérer un tableau d'GeoMatchSetSummary objets	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListIPSets	Accorde l'autorisation de récupérer un tableau d'objets IPSet Summary	List			
ListLoggingConfigurations	Accorde l'autorisation de récupérer un tableau d' LoggingConfiguration objets	List			
ListRateBasedRules	Accorde l'autorisation de récupérer un tableau d' RuleSummary objets	List			
ListRegexMatchSets	Accorde l'autorisation de récupérer un tableau d' RegexMatchSetSummary objets	List			
ListRegexPatternSets	Accorde l'autorisation de récupérer un tableau d' RegexPatternSetSummary objets	List			
ListResourcesForWebACL	Accorde l'autorisation de récupérer un tableau de ressources associées à un élément WebACL spécifié	List	webacl*		
ListRuleGroups	Accorde l'autorisation de récupérer un tableau d' RuleGroup objets	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListRules	Accorde l'autorisation de récupérer un tableau d' RuleSummary objets	List			
ListSizeConstraintSets	Accorde l'autorisation de récupérer un tableau d' SizeConstraintSetSummary objets	List			
ListSqlInjectionMatchSets	Accorde l'autorisation de récupérer un tableau d' SqlInjectionMatchSet objets	List			
ListSubscribedRuleGroups	Accorde l'autorisation de récupérer un tableau d' RuleGroup objets auxquels vous êtes abonné	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource	Lecture	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Accorde l'autorisation de récupérer un tableau d'ACLSummary objets Web	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListXssMatchSets	Accorde l'autorisation de récupérer un tableau d' XssMatchSet objets	List			
PutLoggingConfiguration	Accorde l'autorisation d' LoggingConfiguration associer un à une ACL Web	Écrire	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	Accorde l'autorisation d'attacher une politique IAM à un groupe de règles spécifié afin de prendre en charge le partage de groupes de règles entre les comptes	Gestion des autorisations	rulegroup*		
TagResource	Accorde l'autorisation d'ajouter une balise à une ressource	Balisage	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UntagResource	Accorde l'autorisation de supprimer une balise d'une ressource	Identification	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateByteMatchSet	Accorde l'autorisation d'insérer ou de supprimer ByteMatch Tuple des objets dans un ByteMatchSet	Écrire	bytematchset*		
UpdateGeoMatchSet	Accorde l'autorisation d'insérer ou de supprimer GeoMatchConstraint des objets dans un GeoMatchSet	Écrire	geomatchset*		
UpdateIPSet	Accorde l'autorisation d'insérer ou de supprimer des objets IPSet Descriptor dans un IPSet	Écrire	ipset*		
UpdateRateBasedRule	Accorde l'autorisation d'insérer ou de supprimer des objets de prédicat dans une règle basée sur le taux et de les mettre à jour RateLimit dans la règle	Écrire	ratebasedrule*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRegexMatchSet	Accorde l'autorisation d'insérer ou de supprimer RegexMatchTuple des objets dans un RegexMatchSet	Écrire	regexmatchset*		
UpdateRegexPatternSet	Accorde l'autorisation d'insérer ou de supprimer RegexPatternStrings dans un RegexPatternSet	Écrire	regexpatternset*		
UpdateRule	Accorde l'autorisation d'insérer ou de supprimer des objets Predicate dans un élément Rule	Écrire	rule*		
UpdateRuleGroup	Accorde l'autorisation d'insérer ou de supprimer ActivatedRule des objets dans un RuleGroup	Écrire	rulegroup*		
UpdateSizeConstraintSet	Accorde l'autorisation d'insérer ou de supprimer SizeConstraint des objets dans un SizeConstraintSet	Écrire	sizeconstraintset*		
UpdateSqlInjectionMatchSet	Accorde l'autorisation d'insérer ou de supprimer SqlInjectionMatchTuple des objets dans un SqlInjectionMatchSet	Écrire	sqlinjectionmatchset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateWebACL	Accorde l'autorisation d'insérer ou de supprimer ActivatedRule des objets dans un WebACL	Gestion des autorisations	webacl*		
UpdateXssMatchSet	Accorde l'autorisation d'insérer ou de supprimer XssMatchTuple des objets dans un XssMatchSet	Écrire	xssmatchset*		

Types de ressources définis par AWS WAF Regional

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
bytematchset	`arn:${Partition}:waf-regional:${Region}:${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf-regional:${Region}:${Account}:ipset/${Id}`	
loadbalancer/app/	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/`	

Types de ressources	ARN	Clés de condition
	app/${LoadBalancerName}/${LoadBalancerId}	
ratebasedrule	arn:${Partition}:waf-regional:${Region}:${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf-regional:${Region}:${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf-regional:${Region}:${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf-regional:${Region}:${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf-regional:${Region}:${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf-regional:${Region}:${Account}:geomatchset/${Id}	
rulegroup	arn:${Partition}:waf-regional:${Region}:${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

Clés de condition pour AWS WAF Regional

AWS WAF Regional définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de l'ensemble des valeurs autorisées pour chacune des balises.	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction de la valeur de balise associé à la ressource.	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de balises obligatoires dans la demande.	ArrayOfString

Actions, ressources et clés de condition pour AWS WAF V2

AWS WAF V2 (préfixe de service :`wafv2`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS WAF V2
- Types de ressources définis par AWS WAF V2
- Clés de condition pour AWS WAF V2

Actions définies par AWS WAF V2

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateWebACL	Accorde l'autorisation d'associer un élément WebACL à une ressource	Écriture	webacl*		amplify:AssociateWebACL apigateway:SetWebACL apprunner:AssociateWebAcl appsync:AssociateWebACL appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccess

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					InstanceWebAcl elasticloadbalancing:CreateWebACLAssociation elasticloadbalancing:SetWebAcl wafv2:GetPermissionPolicy wafv2:PutPermissionPolicy
			amplify-app		
			apigateway		
			apprunner		
			appsync		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			loadbalancer/app/		
			userpool		
			verified-access-instance		
CheckCapacity	Accorde l'autorisation de calculer les besoins en unité de capacité ACL web (WCU) pour une étendue et un ensemble de règles spécifiés	Lecture			
CreateAPIKey	Accorde l'autorisation de créer une clé d'API à utiliser dans le cadre de l'intégration de l'API CAPTCHA dans vos applications clientes JavaScript	Écrire			
CreateIPSet	Accorde l'autorisation de créer un IPSet	Écrire	ipset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexPatternSet	Accorde l'autorisation de créer un RegexPatternSet	Écrire	regexpatternset*		wafv2:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Accorde l'autorisation de créer un RuleGroup	Écrire	rulegroup*		wafv2:TagResource
			ipset		
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACL	Accorde l'autorisation de créer un élément WebACL	Écrire	webacl*		wafv2:TagResource
			ipset		
			managedruleset		
			regexpatternset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			rulegroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAPIKey	Accorde l'autorisation de supprimer une clé d'API	Écrire			
DeleteFirewallManagerRuleGroups	Accorde l'autorisation de suppression FirewallManagedRulesGroups depuis un WebACL s'il n'est plus géré par Firewall Manager	Écrire	webacl*		
DeleteIPSet	Accorde l'autorisation de supprimer un IPSet	Écrire	ipset*		
DeleteLoggingConfiguration	Accorde l'autorisation de le supprimer LoggingConfiguration d'un WebACL	Écrire	webacl*		
				wafv2:LogScope	
DeletePermissionPolicy	Accorde l'autorisation de supprimer PermissionPolicy le RuleGroup	Gestion des autorisations	rulegroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRegexPatternSet	Accorde l'autorisation de supprimer un RegexPatternSet	Écrire	regexpatternset*		
DeleteRuleGroup	Accorde l'autorisation de supprimer un RuleGroup	Écrire	rulegroup*		
DeleteWebACL	Accorde l'autorisation de supprimer un élément WebACL	Écrire	webacl*		
DescribeAllManagedProducts	Accorde l'autorisation de récupérer des informations sur le produit pour un groupe de règles gérées	Lecture			
DescribeManagedProductsByVendor	Accorde l'autorisation de récupérer des informations sur le produit pour un groupe de règles gérées par un fournisseur donné	Lecture			
DescribeManagedRuleGroup	Accorde l'autorisation de récupérer des informations de haut niveau pour un groupe de règles géré	Lecture			
DisassociateFirewallManager [autorisation uniquement]	Accorde l'autorisation de dissocier Firewall Manager d'un élément WebACL	Écrire	webacl*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateWebACL	Accorde l'autorisation de dissocier un élément WebACL d'une ressource d'application	Écrire	amplify-app		amplify:DisassociateWebACL apigateway:SetWebACL apprunner:DisassociateWebAcl appsync:DisassociateWebACL appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalanci

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ng:DeleteWebACLAssociation elasticloadbalancing:SetWebAcl wafv2:PutPermissionPolicy
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GenerateMobileSdkReleaseUrl	Accorde l'autorisation de générer une URL de téléchargement présignée pour la version spécifiée du kit SDK mobile.	Lecture			
GetDecryptedAPIKey	Accorde l'autorisation de renvoyer votre clé d'API sous forme déchiffrée. Utilisez ceci pour vérifier les domaines de jeton que vous avez définis pour la clé	Lecture			
GetIPSet	Accorde l'autorisation de récupérer des informations sur un IPSet	Lecture	ipset*		
				aws:ResourceTag/${TagKey}	
GetLoggingConfiguration	Accorde l'autorisation de récupérer LoggingConfiguration pour un WebACL	Lecture	webacl*		
				aws:ResourceTag/${TagKey} wafv2:LogScope	
GetManagedRuleSet	Accorde l'autorisation de récupérer des informations sur un ManagedRuleSet	Lecture	managedruleset*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMobileSdkRelease	Accorde l'autorisation de récupérer des informations pour la version spécifiée du kit SDK mobile, y compris les notes de mise à jour et les étiquettes.	Lecture			
GetPermissionPolicy	Accorde l'autorisation de récupérer un PermissionPolicy pour un RuleGroup	Lecture	rulegroup*		
GetRateBasedStatementManagedKeys	Accorde l'autorisation d'afficher les clés actuellement bloquées par une règle basée sur le taux	Lecture	webacl*		
				aws:ResourceTag/${TagKey}	
GetRegexPatternSet	Accorde l'autorisation de récupérer des informations sur un RegexPatternSet	Lecture	regexpatternset*		
				aws:ResourceTag/${TagKey}	
GetRuleGroup	Accorde l'autorisation de récupérer des informations sur un RuleGroup	Lecture	rulegroup*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSampledRequests	Accorde l'autorisation de récupérer des informations détaillées sur un échantillon de requêtes web	Lecture	webacl*		
GetTopPathStatisticsByTraffic	Accorde l'autorisation de récupérer des statistiques de chemin agrégées avec une analyse du trafic par bot pour une WebACL dans un intervalle de temps spécifié	Lecture	webacl*		
GetWebACL	Accorde l'autorisation de récupérer des détails sur un élément WebACL	Lecture	webacl*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWebACLForResource	Accorde l'autorisation de récupérer l'élément WebACL associé à une ressource	Lecture	webacl*		amplify:GetWebACLForResource apprunner:DescribeWebAclForService appsync:GetWebACLForResource cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl elasticloadbalancing:GetLoadBalancerWebACL

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					wafv2:GetWebACL
			amplify-app		
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
ListAPIKeys	Accorde l'autorisation de récupérer une liste des clés d'API que vous avez définies pour la portée spécifiée	List			
ListAvailableManagedRuleGroupVersions	Accorde l'autorisation de récupérer un tableau des versions de groupes de règles gérés que vous pouvez utiliser	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAvailableManagedRuleGroups	Accorde l'autorisation de récupérer un tableau des groupes de règles gérés que vous pouvez utiliser	List			
ListIPSets	Accorde l'autorisation de récupérer un tableau d'objets IPSet Summary pour les ensembles d'adresses IP que vous gérez	List			
ListLoggingConfigurations	Accorde l'autorisation de récupérer un tableau de vos LoggingConfiguration objets	List		wafv2:LogScope	
ListManagedRuleSets	Accorde l'autorisation de récupérer un tableau de vos ManagedRuleSet objets	List			
ListMobileSdkReleases	Accorde l'autorisation de récupérer la liste des versions disponibles pour le kit SDK mobile et la plateforme des appareils spécifiée.	List			
ListRegexPatternSets	Accorde l'autorisation de récupérer un tableau d' RegexPatternSetSummary objets pour les ensembles de modèles regex que vous gérez	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListResourcesForWebACL	Accorde l'autorisation de récupérer un tableau des Amazon Resource Names (ARNs) pour les ressources associées à une ACL Web	List	webacl*		amplify:ListResourcesForWebACL apprunner:ListAssociatedServicesForWebAcl appsync:ListResourcesForWebACL cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations elasticloadbalancing:DescribeWebACLA

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					ssociation
			amplify-app		
			apprunner		
			userpool		
			verified-access-instance		
ListRuleGroups	Accorde l'autorisation de récupérer un tableau d' RuleGroupSummary objets pour les groupes de règles que vous gérez	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListWebACLs	Accorde l'autorisation de récupérer un tableau d'ACLSummary objets Web pour le Web ACLs que vous gérez	List			
PutFirewallManagerRuleGroups [autorisation uniquement]	Accorde l'autorisation de créer FirewallManagedRulesGroups dans un WebACL	Écrire	webacl*		
PutLoggingConfiguration	Accorde l'autorisation d'activer une LoggingConfiguration, de démarrer la journalisation pour une ACL Web	Écrire	webacl*		iam:CreateServiceLinkedRole
				wafv2:LogScope wafv2:LogDestinationResource	
PutManagedRuleSetVersions	Accorde l'autorisation d'activer , de créer une nouvelle version ou de mettre à jour une version existante d'un ManagedRuleSet	Écrire	managedruleset*		
			rulegroup* –		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutPermissionPolicy	Accorde l'autorisation d'attacher une politique IAM à une ressource, utilisée pour partager des groupes de règles entre des comptes	Gestion des autorisations	rulegroup*		
TagResource	Accorde l'autorisation d'associer des balises à une AWS ressource	Identification	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de dissocier les balises d'une ressource AWS	Identification	ipset		
			regexpatternset		
			rulegroup		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			webacl		
				aws:TagKeys	
UpdateIPSet	Accorde l'autorisation de mettre à jour un IPSet	Écrire	ipset*		
				aws:ResourceTag/${TagKey}	
UpdateManagedRuleSetVersionExpiryDate	Autorise la mise à jour de la date d'expiration d'une version dans ManagedRuleSet	Écrire	managedruleset*		
UpdateRegexPatternSet	Accorde l'autorisation de mettre à jour un RegexPatternSet	Écrire	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	Accorde l'autorisation de mettre à jour un RuleGroup	Écrire	rulegroup*		
			ipset		
			regexpatternset		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
UpdateWebACL	Accorde l'autorisation de mettre à jour un élément WebACL	Écrire	webacl*		
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS WAF V2

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
webacl	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}	aws:ResourceTag/${TagKey}
ipset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/ipset/${Name}/${Id}	aws:ResourceTag/${TagKey}
managedruleset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/managedruleset/${Name}/${Id}	
rulegroup	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/rulegroup/${Name}/${Id}	aws:ResourceTag/${TagKey}
regexpatternset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/regexpatternset/${Name}/${Id}	aws:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
apigateway	arn:${Partition}:apigateway:${Region}::/restapis/${ApiId}/stages/${StageName}	
appsync	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}	
userpool	arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}	

Types de ressources	ARN	Clés de condition
apprunner	`arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}`	
verified-access-instance	`arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`	
amplify-app	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}`	

Clés de condition pour AWS WAF V2

AWS WAF V2 définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de l'ensemble de valeurs autorisées pour chacune des identifications	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction de la valeur d'identification associée à la ressource	String
aws:TagKeys	Filtre l'accès en fonction de la présence de identifications obligatoires dans la demande	ArrayOfString

Clés de condition	Description	Type
wafv2:LogDestinationResource	Filtre l'accès par ARN de destination du journal pour PutLoggingConfiguration l'API	ARN
wafv2:LogScope	Filtre l'accès par étendue du journal pour l'API de configuration de journalisation	String

Actions, ressources et clés de condition pour AWS Well-Architected Tool

AWS Well-Architected Tool (préfixe de service `wellarchitected` :) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Well-Architected Tool
- Types de ressources définis par AWS Well-Architected Tool
- Clés de condition pour AWS Well-Architected Tool

Actions définies par AWS Well-Architected Tool

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate Lenses	Accorde l'autorisation d'associer un cadre à la charge de travail spécifiée	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
Associate Profiles	Accorde l'autorisation d'associer un profil à la charge de travail spécifiée	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
Configure Integration [autorisation uniquement]	Accorde l'autorisation de configurer l'intégration	Écrire			
CreateLensShare	Autorise le propriétaire d'un objectif à le partager avec d'autres AWS comptes et utilisateurs d'IAM	Écrire	lens*		
				aws:ResourceTag/${TagKey}	
CreateLensVersion	Accorde l'autorisation de créer une version de cadre	Écrire	lens*		
				aws:ResourceTag/${TagKey}	
CreateMilestone	Accorde l'autorisation de créer un jalon pour la charge de travail spécifiée	Écrire	workload*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
CreateProfile	Accorde l'autorisation de créer un nouveau profil	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileShare	Autorise le propriétaire d'un profil à le partager avec d'autres AWS comptes et utilisateurs IAM	Écrire	profile*		
				aws:ResourceTag/${TagKey}	
CreateReviewTemplate	Accorde l'autorisation de créer un nouveau modèle de révision	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateShare	Autorise le propriétaire d'un modèle d'évaluation à le partager avec d'autres AWS comptes et utilisateurs IAM	Écrire	review-template*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkload	Accorde l'autorisation de créer une charge de travail	Écriture		aws:RequestTag/${TagKey} aws:TagKeys wellarchitected:JiraProjectKey	
CreateWorkloadShare	Accorde l'autorisation de partager une charge globale avec un autre compte	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
DeleteLens	Accorde l'autorisation de supprimer un cadre	Écrire	lens*		
				aws:ResourceTag/${TagKey}	
DeleteLensShare	Accorde l'autorisation de supprimer un partage de cadre existant	Écrire	lens*		
				aws:ResourceTag/${TagKey}	
DeleteProfile	Accorde l'autorisation de supprimer un profil.	Écrire	profile*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DeleteProfileShare	Accorde l'autorisation de supprimer un partage de profil existant	Écrire	profile*		
				aws:ResourceTag/${TagKey}	
DeleteReviewTemplate	Accorde l'autorisation de supprimer un modèle de révision existant	Écrire	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteTemplateShare	Accorde l'autorisation de supprimer un partage de modèle de révision existant	Écrire	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteWorkload	Accorde l'autorisation de supprimer une charge de travail existante	Écriture	workload*		
				aws:ResourceTag/${TagKey}	
DeleteWorkloadShare	Accorde l'autorisation de supprimer un partage de charge de travail existant	Écriture	workload*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
DisassociateLenses	Accorde l'autorisation de dissocier un cadre de la charge de travail spécifiée	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
DisassociateProfiles	Accorde l'autorisation de dissocier un profil de la charge de travail spécifiée	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
ExportLens	Accorde l'autorisation d'exporter un cadre existant	Lecture	lens*		
				aws:ResourceTag/${TagKey}	
GetAnswer	Accorde l'autorisation de récupérer la réponse spécifiée à partir de l'examen de cadre spécifié	Lecture	workload*		
				aws:ResourceTag/${TagKey}	
GetConsolidatedReport	Accorde l'autorisation d'obtenir les mesures du rapport consolidé ou de générer le rapport consolidé au format PDF dans ce compte	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetGlobalSettings	Accorde l'autorisation d'obtenir tous les paramètres du compte	Lecture			
GetLens	Accorde l'autorisation d'obtenir un cadre existant	Lecture	lens*		
				aws:ResourceTag/${TagKey}	
GetLensReview	Accorde l'autorisation d'extraire l'examen de cadre spécifié de la charge de travail spécifiée	Lecture	workload*		
				aws:ResourceTag/${TagKey}	
GetLensReviewReport	Accorde l'autorisation de récupérer le rapport de l'examen d'un cadre	Lecture	workload*		
				aws:ResourceTag/${TagKey}	
GetLensVersionDifference	Accorde l'autorisation d'obtenir la différence entre la version de cadre spécifiée et la dernière version de cadre disponible	Lecture	lens*		
				aws:ResourceTag/${TagKey}	
GetMilestone	Accorde l'autorisation de récupérer le jalon spécifié de la charge de travail spécifiée	Lecture	workload*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetProfile	Accorde l'autorisation de récupérer la profil spécifié	Lecture	profile*		
				aws:ResourceTag/${TagKey}	
GetProfileTemplate	Accorde l'autorisation de récupérer le modèle de profil spécifié	Lecture			
GetReviewTemplate	Accorde l'autorisation de récupérer le modèle de révision spécifié	Lecture	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateAnswer	Accorde l'autorisation de récupérer la réponse spécifiée à partir de l'examen de cadre de modèle de révision spécifié	Lecture	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateLensReview	Accorde l'autorisation de récupérer l'examen de cadre spécifié du modèle de révision spécifié	Lecture	review-template*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetWorkload	Accorde l'autorisation de récupérer la charge de travail spécifiée	Lecture	workload*		
				aws:ResourceTag/${TagKey}	
ImportLens	Accorde l'autorisation d'importer un nouveau cadre	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
ListAnswers	Accorde l'autorisation de répertorier les réponses de l'examen de cadre spécifié	List	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckDetails	Accorde l'autorisation de répertorier les informations de chèque de la charge de travail	List	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckSummaries	Accorde l'autorisation de répertorier les récapitulatifs de chèque de la charge de travail	List	workload*		
				aws:ResourceTag/${TagKey}	
ListLensReviewImprovements	Accorde l'autorisation de répertorier les améliorations de l'examen du cadre spécifié	Liste	workload*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
ListLensReviews	Accorde l'autorisation de répertorier les examens de cadre de la charge de travail spécifiée	List	workload*		
				aws:ResourceTag/${TagKey}	
ListLensShares	Accorde l'autorisation de répertorier tous les partages créés pour un cadre	List	lens*		
				aws:ResourceTag/${TagKey}	
ListLenses	Accorde l'autorisation de répertorier les cadres disponibles du compte	Liste			
ListMilestones	Accorde l'autorisation de répertorier les jalons de la charge de travail spécifiée	Liste	workload*		
				aws:ResourceTag/${TagKey}	
ListNotifications	Accorde l'autorisation de répertorier les notifications liées au compte ou à la ressource spécifiée	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListProfileNotifications	Accorde l'autorisation de répertorier les notifications du profil liées à la ressource spécifiée	List			
ListProfileShares	Accorde l'autorisation de répertorier tous les partages créés pour un profil	List	profile*		
				aws:ResourceTag/${TagKey}	
ListProfiles	Accorde l'autorisation de répertorier les profils disponibles du compte	List			
ListReviewTemplateAnswers	Accorde l'autorisation de répertorier les réponses de l'examen de cadre de modèle de révision spécifié	List	review-template*		
				aws:ResourceTag/${TagKey}	
ListReviewTemplates	Accorde l'autorisation de répertorier les modèles de révision disponibles pour le compte	List			
ListShareInvitations	Accorde l'autorisation de répertorier les invitations de partage de charge de travail du compte ou de l'utilisateur spécifié	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource Well-Architected	Lecture	lens		
			profile		
			review-template		
			workload		
				aws:ResourceTag/${TagKey}	
ListTemplateShares	Accorde l'autorisation de répertorier tous les partages créés pour un modèle de révision	List	review-template*		
				aws:ResourceTag/${TagKey}	
ListWorkloadShares	Accorde l'autorisation de répertorier les partages de la charge travail spécifiée	Liste	workload*		
				aws:ResourceTag/${TagKey}	
ListWorkloads	Accorde l'autorisation de répertorier les charges de travail dans le compte	Liste			
TagResource	Accorde l'autorisation de baliser une ressource Well-Architected	Balisage	lens		
			profile		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			review-template		
			workload		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation d'annuler le balisage d'une ressource Well-Architected	Balisage	lens		
			profile		
			review-template		
			workload		
				aws:TagKeys	
UpdateAnswer	Accorde l'autorisation de mettre à jour les propriétés de la réponse spécifiée	Écrire	workload*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateGlobalSettings	Accorde l'autorisation de gérer tous les paramètres du compte	Écrire		wellarchitected:JiraProjectKey	
UpdateIntegration	Autorise la mise à jour des propriétés de l'intégration	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
UpdateLensReview	Accorde l'autorisation de mettre à jour les propriétés de l'examen de cadre spécifié	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
UpdateProfile	Accorde l'autorisation de mettre à jour les propriétés du profil spécifié	Écrire	profile*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplate	Accorde l'autorisation de mettre à jour les propriétés du modèle de révision spécifié	Écrire	review-template*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateReviewTemplateAnswer	Accorde l'autorisation de mettre à jour les propriétés de la réponse au modèle de révision spécifiée	Écrire	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplateLensReview	Accorde l'autorisation de mettre à jour les propriétés de l'examen de cadre de modèle de révision spécifié	Écrire	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateShareInvitation	Accorde l'autorisation de mettre à jour le statut de l'invitation de partage de charge de travail spécifiée	Écriture			
UpdateWorkload	Accorde l'autorisation de mettre à jour les propriétés de la charge travail spécifiée	Écrire	workload*		
				aws:ResourceTag/${TagKey} wellarchitected:JiraProjectKey	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateWorkloadShare	Accorde l'autorisation de mettre à jour les propriétés du partage de charge de travail spécifié	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
UpgradeLensReview	Accorde l'autorisation de mettre à niveau l'examen de cadre spécifié pour utiliser la dernière version du cadre associé	Écrire	workload*		
				aws:ResourceTag/${TagKey}	
UpgradeProfileVersion	Accorde l'autorisation de mettre à niveau la charge de travail spécifiée pour utiliser la dernière version du profil associé	Écrire	profile*		
			workload*		
				aws:ResourceTag/${TagKey}	
UpgradeReviewTemplateLensReview	Accorde l'autorisation de mettre à niveau l'examen de cadre spécifié du modèle de révision spécifié	Écrire	review-template*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par AWS Well-Architected Tool

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut

également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
workload	`arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}`	aws:ResourceTag/${TagKey}
lens	`arn:${Partition}:wellarchitected:${Region}:${Account}:lens/${ResourceId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:wellarchitected:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
review-template	`arn:${Partition}:wellarchitected:${Region}:${Account}:review-template/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Well-Architected Tool

AWS Well-Architected Tool définit les clés de condition suivantes qui peuvent être utilisées dans `Condition` l'élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de balise dans la requête.	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource.	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une requête	ArrayOfString
wellarchitected:JiraProjectKey	Filtre l'accès par clé de projet	String

Actions, ressources et clés de condition pour AWS Wickr

AWS Wickr (préfixe de service :`wickr`) fournit les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS Wickr
- Types de ressources définis par AWS Wickr
- Clés de condition pour AWS Wickr

Actions définies par AWS Wickr

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchCreateUser	Accorde l'autorisation de créer des utilisateurs par lots dans un réseau Wickr	Écrire	network*		
BatchDeleteUser	Accorde l'autorisation de supprimer par lots des utilisateurs d'un réseau Wickr	Écrire	network*		
BatchLookupUserUname	Autorise la recherche par lots de noms d'utilisateurs dans un réseau Wickr	Lecture	network*		
BatchReinviteUser	Accorde l'autorisation de réinviter par lots des utilisateurs dans un réseau Wickr	Écrire	network*		
BatchResetDevicesForUser	Accorde l'autorisation de réinitialiser par lots les appareils d'un utilisateur d'un réseau Wickr	Écrire	network*		
BatchToggleUserSuspendStatus	Accorde l'autorisation de changer par lots le statut de suspension d'un utilisateur dans un réseau Wickr	Écrire	network*		
CreateAdminSession	Accorde l'autorisation de créer et de gérer des réseaux Wickr	Écrire	network*		
CreateBot	Accorde l'autorisation de créer un bot dans un réseau Wickr	Écrire	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateDataRetentionBot	Autorise la création d'un bot de conservation des données dans un réseau Wickr	Écrire	network*		
CreateDataRetentionBotChallenge	Autorise la création d'un défi de bot de conservation des données dans un réseau Wickr	Écrire	network*		
CreateNetwork	Autorise la création d'un nouveau réseau Wickr	Écrire	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSecurityGroup	Accorde l'autorisation de créer un groupe de sécurité dans un réseau Wickr	Écrire	network*		
DeleteBot	Accorde l'autorisation de supprimer un bot d'un réseau Wickr	Écrire	network*		
DeleteDataRetentionBot	Accorde l'autorisation de supprimer un bot de conservation des données d'un réseau Wickr	Écrire	network*		
DeleteNetwork	Autorise la suppression des réseaux Wickr	Écrire	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSecurityGroup	Accorde l'autorisation de supprimer un groupe de sécurité d'un réseau Wickr	Écrire	network*		
GetBot	Accorde l'autorisation d'obtenir des informations sur les robots dans un réseau Wickr	Lecture	network*		
GetBotsCount	Accorde l'autorisation d'obtenir le nombre de bots pour un réseau Wickr	Lecture	network*		
GetDataRetentionBot	Accorde l'autorisation d'obtenir des informations sur le bot de conservation des données dans un réseau Wickr	Lecture	network*		
GetGuestUserHistoryCount	Accorde l'autorisation d'obtenir le compte de l'historique des utilisateurs invités pour un réseau Wickr	Lecture	network*		
GetNetwork	Accorde l'autorisation d'obtenir les détails d'un réseau Wickr	Lecture	network*		
GetNetworkSettings	Accorde l'autorisation d'obtenir les paramètres réseau d'un réseau Wickr	Lecture	network*		
GetOidcInfo	Accorde l'autorisation d'obtenir des informations OIDC pour un réseau Wickr	Lecture	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSecurityGroup	Accorde l'autorisation d'obtenir des informations sur un groupe de sécurité dans un réseau Wickr	Lecture	network*		
GetUser	Accorde l'autorisation d'obtenir des informations sur un utilisateur dans un réseau Wickr	Lecture	network*		
GetUsersCount	Accorde l'autorisation d'obtenir le nombre d'utilisateurs pour un réseau Wickr	Lecture	network*		
ListBlockedGuestUsers	Accorde l'autorisation de répertorier les utilisateurs invités bloqués dans un réseau Wickr	Lecture	network*		
ListBots	Accorde l'autorisation de répertorier les robots dans un réseau Wickr	Lecture	network*		
ListDevicesForUser	Accorde l'autorisation de répertorier les appareils d'un utilisateur dans un réseau Wickr	Lecture	network*		
ListGuestUsers	Accorde l'autorisation de répertorier les utilisateurs invités dans un réseau Wickr	Lecture	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListNetworks	Permet de répertorier les réseaux Wickr	Lecture			
ListSecurityGroupUsers	Accorde l'autorisation de répertorier les utilisateurs d'un groupe de sécurité dans un réseau Wickr	Lecture	network*		
ListSecurityGroups	Accorde l'autorisation de répertorier les groupes de sécurité dans un réseau Wickr	Lecture	network*		
ListTagsForResource	Octroie l'autorisation de répertorier les balises appliquées à une ressource Wickr	Lecture	network*		
ListUsers	Accorde l'autorisation de répertorier les utilisateurs d'un réseau Wickr	Lecture	network*		
RegisterOidcConfig	Accorde l'autorisation d'enregistrer la configuration OIDC pour un réseau Wickr	Écrire	network*		
RegisterOidcConfigTest	Accorde l'autorisation de tester la configuration OIDC pour un réseau Wickr	Écrire	network*		
TagResource	Accorde l'autorisation d'ajouter des tags à une ressource Wickr spécifiée	Identification	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de dissocier les balises spécifiées de la ressource Wickr spécifiée	Identification	network*		
				aws:TagKeys	
UpdateBot	Accorde l'autorisation de mettre à jour un bot dans un réseau Wickr	Écrire	network*		
UpdateDataRetention	Autorise la mise à jour des paramètres de conservation des données dans un réseau Wickr	Écrire	network*		
UpdateGuestUser	Accorde l'autorisation de mettre à jour le statut d'utilisateur invité dans un réseau Wickr	Écrire	network*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNetworkDetails	Octroie l'autorisation de mettre à jour les informations d'un réseau Wickr	Écrire	network*		
UpdateNetworkSettings	Accorde l'autorisation de mettre à jour les paramètres réseau d'un réseau Wickr	Écrire	network*		
UpdateSecurityGroup	Accorde l'autorisation de mettre à jour un groupe de sécurité dans un réseau Wickr	Écrire	network*		
UpdateUser	Accorde l'autorisation de mettre à jour les informations utilisateur dans un réseau Wickr	Écrire	network*		

Types de ressources définis par AWS Wickr

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
network	`arn:${Partition}:wickr:${Region}:${Account}:network/${NetworkId}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS Wickr

AWS Wickr définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction de la clé et la valeur d'une balise dans une demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification dans une demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon WorkDocs

Amazon WorkDocs (préfixe de service :`workdocs`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkDocs
- Types de ressources définis par Amazon WorkDocs
- Clés de condition pour Amazon WorkDocs

Actions définies par Amazon WorkDocs

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AbortDocumentVersionUpload	Accorde l'autorisation d'abandonner le téléchargement de la version de document spécifiée qui a été précédemment lancé par InitiateDocumentVersionUpload	Écrire			
ActivateUser	Accorde l'autorisation d'activer l'utilisateur spécifié. Seuls les utilisateurs actifs peuvent accéder à Amazon WorkDocs	Écrire			
AddNotificationPermissions [autorisation uniquement]	Accorde l'autorisation d'ajouter des principaux autorisés à s'abonner aux notifications d'appel APIs pour un site donné WorkDocs	Écrire			
AddResourcePermissions	Accorde l'autorisation de créer un jeu d'autorisations pour le dossier ou document spécifié	Écrire			
AddUserToGroup	Accorde l'autorisation d'ajouter un utilisateur à un groupe	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
[autorisation uniquement]					
CheckAlias [autorisation uniquement]	Accorde l'autorisation de vérifier un alias	Lecture			
CreateComment	Accorde l'autorisation d'ajouter un nouveau commentaire à la version du document spécifiée	Écrire			
CreateCustomMetadata	Accorde l'autorisation d'ajouter une ou plusieurs propriétés personnalisées à la ressource spécifiée	Écrire			
CreateFolder	Accorde l'autorisation de créer un dossier avec le nom spécifié et le dossier parent	Écrire			
CreateInstance [autorisation uniquement]	Accorde l'autorisation de créer une instance	Écrire			
CreateLabels	Accorde l'autorisation d'ajouter des étiquettes à la ressource donnée	Écrire			
CreateNotificationSubscription	Accorde l'autorisation de configurer WorkDocs pour utiliser les notifications Amazon SNS	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUser	Accorde l'autorisation de créer un utilisateur dans un répertoire Simple AD ou Microsoft AD	Écrire			
DeactivateUser	Accorde l'autorisation de désactiver l'utilisateur spécifié, ce qui révoque l'accès de l'utilisateur à Amazon WorkDocs	Écrire			
DeleteComment	Accorde l'autorisation de supprimer le commentaire spécifié de la version du document	Écrire			
DeleteCustomMetadata	Accorde l'autorisation de supprimer les métadonnées personnalisées de la ressource spécifiée	Écrire			
DeleteDocument	Accorde l'autorisation de supprimer définitivement le document spécifié et ses métadonnées associées	Écrire			
DeleteDocumentVersion	Accorde l'autorisation de supprimer les versions d'un document spécifié	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteFolder	Accorde l'autorisation de supprimer définitivement le dossier spécifié et son contenu	Écrire			
DeleteFolderContents	Accorde l'autorisation de supprimer le contenu du dossier spécifié	Écrire			
DeleteInstance [autorisation uniquement]	Accorde l'autorisation de supprimer une instance	Écrire			
DeleteLabels	Accorde l'autorisation de supprimer une ou plusieurs étiquettes d'une ressource	Écrire			
DeleteNotificationPermissions [autorisation uniquement]	Accorde l'autorisation de supprimer les principaux autorisés à s'abonner aux notifications d'appel APIs pour un site donné WorkDocs	Écrire			
DeleteNotificationSubscription	Accorde l'autorisation de supprimer l'abonnement spécifié de l'organisation spécifiée	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteUser	Accorde l'autorisation de supprimer l'utilisateur spécifié d'un répertoire Simple AD ou Microsoft AD	Écrire			
DeregisterDirectory [autorisation uniquement]	Accorde l'autorisation d'annuler l'enregistrement d'un répertoire	Écrire			
DescribeActivities	Accorde l'autorisation de récupérer les activités d'un utilisateur dans un laps de temps donné	List			
DescribeAvailableDirectories [autorisation uniquement]	Accorde l'autorisation de décrire les répertoires disponibles	List			
DescribeComments	Accorde l'autorisation de répertorier tous les commentaires pour la version de document spécifiée	List			
DescribeDocumentVersions	Accorde l'autorisation de récupérer les versions de document pour le document spécifié	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeFolderContents	Accorde l'autorisation de décrire le contenu du dossier spécifié, y compris ses documents et sous-dossiers	List			
DescribeGroups	Accorde l'autorisation de décrire les groupes d'utilisateurs	List			
DescribeInstanceExports [autorisation uniquement]	Accorde l'autorisation de décrire l'historique des exportations pour une instance	List			
DescribeInstances [autorisation uniquement]	Accorde l'autorisation de décrire les instances	List			
DescribeNotificationPermissions [autorisation uniquement]	Accorde l'autorisation de décrire les principaux autorisés à s'abonner aux notifications d'appel APIs pour un site donné WorkDocs	List			
DescribeNotificationSubscriptions	Accorde l'autorisation de répertorier les abonnements de notification spécifiés	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeResourcePermissions	Accorde l'autorisation d'afficher une description des autorisations de ressource spécifiées	List			
DescribeRootFolders	Accorde l'autorisation de décrire les dossiers racine	List			
DescribeUsers	Accorde l'autorisation d'afficher une description des utilisateurs spécifiés. Vous pouvez décrire tous les utilisateurs ou filtrer les résultats (par exemple, par statut ou organisation)	List			
DownloadDocumentVersion [autorisation uniquement]	Accorde l'autorisation de télécharger une version de document spécifiée	Lecture			
GetCurrentUser	Accorde l'autorisation de récupérer les détails de l'utilisateur actuel	Lecture			
GetDocument	Accorde l'autorisation de récupérer l'objet de document spécifié	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDocumentPath	Accorde l'autorisation de récupérer les informations de chemin (la hiérarchie du dossier racine) pour le document demandé	Lecture			
GetDocumentVersion	Accorde l'autorisation de récupérer la version des métadonnées du document spécifié	Lecture			
GetFolder	Accorde l'autorisation de récupérer les métadonnées du dossier spécifié	Lecture			
GetFolderPath	Accorde l'autorisation de récupérer les informations de chemin (la hiérarchie du dossier racine) pour le dossier spécifié	Lecture			
GetGroup [autorisation uniquement]	Accorde l'autorisation de récupérer des détails pour le groupe spécifié	Lecture			
GetResources	Accorde l'autorisation d'obtenir une collection de ressources	Lecture			
InitiateDocumentVersionUpload	Accorde l'autorisation de créer un nouvel objet de document et un nouvel objet de version	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RegisterDirectory [autorisation uniquement]	Accorde l'autorisation d'enregistrer un répertoire	Écrire			
RemoveAllResourcePermissions	Accorde l'autorisation de supprimer toutes les autorisations de la ressource spécifiée	Écrire			
RemoveResourcePermission	Accorde l'autorisation de supprimer l'autorisation pour le principal spécifié de la ressource indiquée	Écrire			
RestoreDocumentVersions	Accorde l'autorisation de restaurer les versions d'un document spécifié	Écrire			
SearchResources	Accorde l'autorisation de rechercher les métadonnées et le contenu des ressources	List			
StartInstanceExport [autorisation uniquement]	Accorde l'autorisation de démarrer une exportation pour une instance	Écrire	organization*		
UpdateDocument	Accorde l'autorisation de mettre à jour les attributs spécifiés du document spécifié	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateDocumentVersion	Accorde l'autorisation de modifier l'état de la version de document en ACTIVE	Écrire			
UpdateFolder	Accorde l'autorisation de mettre à jour les attributs spécifiés du dossier spécifié	Écrire			
UpdateInstanceAlias [autorisation uniquement]	Accorde l'autorisation de mettre à jour un alias d'instance	Écrire			
UpdateUser	Accorde l'autorisation de mettre à jour les attributs spécifiés de l'utilisateur spécifié, et accorde ou révoque les privilèges administratifs au site Amazon WorkDocs	Écrire			
UpdateUserAdministrativeSettings [autorisation uniquement]	Octroie l'autorisation de mettre à jour les paramètres administratifs d'un utilisateur.	Écrire			

Types de ressources définis par Amazon WorkDocs

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie

les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
organization	`arn:${Partition}:workdocs:${Region}:${Account}:organization/${ResourceId}`	

Clés de condition pour Amazon WorkDocs

WorkDocs ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon WorkLink

Amazon WorkLink (préfixe de service :`worklink`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkLink
- Types de ressources définis par Amazon WorkLink
- Clés de condition pour Amazon WorkLink

Actions définies par Amazon WorkLink

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateDomain	Accorde l'autorisation d'associer un domaine à une WorkLink flotte Amazon	Écrire	fleet*		
AssociateWebsiteAuthorizationProvider	Accorde l'autorisation d'associer un fournisseur d'autorisation de site Web à une WorkLink flotte Amazon	Écrire	fleet*		
AssociateWebsiteCertificateAuthority	Accorde l'autorisation d'associer l'autorité de certification d'un site Web à une WorkLink flotte Amazon	Écrire	fleet*		
CreateFleet	Accorde l'autorisation de créer une WorkLink flotte Amazon	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFleet	Autorise la suppression d'une WorkLink flotte Amazon	Écrire	fleet*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
DescribeAuditStreamConfiguration	Accorde l'autorisation de décrire la configuration du flux d'audit pour une WorkLink flotte Amazon	Lecture	fleet*		
DescribeCompanyNetworkConfiguration	Accorde l'autorisation de décrire la configuration réseau de l'entreprise pour une WorkLink flotte Amazon	Lecture	fleet*		
DescribeDevice	Accorde l'autorisation de décrire les détails d'un appareil associé à une WorkLink flotte Amazon	Lecture	fleet*		
DescribeDevicePolicyConfiguration	Accorde l'autorisation de décrire la configuration de la politique des appareils pour une WorkLink flotte Amazon	Lecture	fleet*		
DescribeDomain	Accorde l'autorisation de décrire les détails d'un domaine associé à une WorkLink flotte Amazon	Lecture	fleet*		
DescribeFleetMetadata	Accorde l'autorisation de décrire les métadonnées d'une WorkLink flotte Amazon	Lecture	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIdentityProviderConfiguration	Accorde l'autorisation de décrire la configuration du fournisseur d'identité pour une WorkLink flotte Amazon	Lecture	fleet*		
DescribeWebsiteCertificateAuthority	Accorde l'autorisation de décrire l'autorité de certification d'un site Web associée à une WorkLink flotte Amazon	Lecture	fleet*		
DisassociateDomain	Accorde l'autorisation de dissocier un domaine d'une flotte Amazon WorkLink	Écrire	fleet*		
DisassociateWebsiteAuthorizationProvider	Accorde l'autorisation de dissocier un fournisseur d'autorisation de site Web d'une flotte Amazon WorkLink	Écrire	fleet*		
DisassociateWebsiteCertificateAuthority	Accorde l'autorisation de dissocier l'autorité de certification d'un site Web d'une flotte Amazon WorkLink	Écrire	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListDevices	Accorde l'autorisation de répertorier les appareils associés à une WorkLink flotte Amazon	List	fleet*		
ListDomains	Accorde l'autorisation de répertorier les domaines associés à une WorkLink flotte Amazon	List	fleet*		
ListFleets	Accorde l'autorisation de répertorier les WorkLink flottes Amazon associées au compte	List			
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource.	Lecture	fleet*		
ListWebsiteAuthorizationProviders	Accorde l'autorisation de répertorier les fournisseurs d'autorisation de sites Web pour une WorkLink flotte Amazon	List	fleet*		
ListWebsiteCertificateAuthorities	Accorde l'autorisation de répertorier les autorités de certification de sites Web associées à une WorkLink flotte Amazon	List	fleet*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
RestoreDomainAccess	Autorise le rétablissement de l'accès à un domaine associé à une WorkLink flotte Amazon	Écrire	fleet*		
RevokeDomainAccess	Accorde l'autorisation de révoquer l'accès à un domaine associé à une flotte Amazon WorkLink	Écrire	fleet*		
SearchEntity [autorisation uniquement]	Accorde l'autorisation de répertorier les appareils d'une WorkLink flotte Amazon	List	fleet*		
SignOutUser	Accorde l'autorisation de déconnecter un utilisateur d'une WorkLink flotte Amazon	Écrire	fleet*		
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une ressource	Balisage	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Identification	fleet*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAuditStreamConfiguration	Autorise la mise à jour de la configuration du flux d'audit pour une WorkLink flotte Amazon	Écrire	fleet*		
UpdateCompanyNetworkConfiguration	Autorise la mise à jour de la configuration réseau de l'entreprise pour une WorkLink flotte Amazon	Écrire	fleet*		
UpdateDevicePolicyConfiguration	Accorde l'autorisation de mettre à jour la configuration de la politique relative aux appareils pour une WorkLink flotte Amazon	Écrire	fleet*		
UpdateDomainMetadata	Accorde l'autorisation de mettre à jour les métadonnées d'un domaine associé à une WorkLink flotte Amazon	Écrire	fleet*		
UpdateFleetMetadata	Autorise la mise à jour des métadonnées d'une WorkLink flotte Amazon	Écrire	fleet*		
UpdateIdentityProviderConfiguration	Accorde l'autorisation de mettre à jour la configuration du fournisseur d'identité pour une WorkLink flotte Amazon	Écrire	fleet*		

Types de ressources définis par Amazon WorkLink

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
fleet	`arn:${Partition}:worklink::${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon WorkLink

Amazon WorkLink définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre les actions en fonction de la présence de paires clé-valeur d'identification dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre les actions en fonction des paires clé-valeur d'identification attachées à la ressource	Chaîne
aws:TagKeys	Filtre les actions en fonction de la présence de clés d'identification dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon WorkMail

Amazon WorkMail (préfixe de service :`workmail`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkMail
- Types de ressources définis par Amazon WorkMail
- Clés de condition pour Amazon WorkMail

Actions définies par Amazon WorkMail

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un

astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AllowVendedLogDeliveryForResource [autorisation uniquement]	Accorde l'autorisation de configurer la livraison des journaux vendus pour les journaux WorkMail d'audit	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateDelegateToResource	Accorde l'autorisation d'ajouter un membre (utilisateur ou groupe) à l'ensemble de délégués de la ressource.	Écriture	organization*		
AssociateMemberToGroup	Accorde l'autorisation d'ajouter un membre (utilisateur ou groupe) à l'ensemble du groupe	Écrire	organization*		
AssumeImpersonationRole	Accorde l'autorisation d'assumer un rôle d'usurpation d'identité pour l'organisation Amazon donnée WorkMail	Écrire	organization*		
				workmail:ImpersonationRoleId	
CancelMailboxExportJob	Accorde l'autorisation d'annuler une tâche d'exportation de boîte aux lettres en cours d'exécution	Écrire	organization*		
CreateAlias	Accorde l'autorisation d'ajouter un alias à l'ensemble d'un membre donné (utilisateur ou groupe) de WorkMail	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateAvailabilityConfiguration	Accorde l'autorisation de créer un nom AvailabilityConfiguration pour l' WorkMail organisation et le domaine Amazon concernés	Écrire	organization*		
CreateGroup	Accorde l'autorisation de créer un groupe qui peut être utilisé WorkMail en appelant l' RegisterToWorkMail opération	Écrire	organization*		
CreateIdentityCenterApplication	Accorde l'autorisation de créer une application Identity Center pour WorkMail	Écrire			
CreateImpersonationRole	Accorde l'autorisation de créer un rôle d'usurpation d'identité pour l'organisation Amazon donnée WorkMail	Écrire	organization*		
CreateInboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de créer une règle de flux de messagerie entrant qui s'applique à tous les messages envoyés à une organisation	Écriture	organization*		
CreateMailDomain [autorisation uniquement]	Accorde l'autorisation de créer un domaine de messagerie.	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateMobileDeviceAccessRule	Accorde l'autorisation de créer une règle d'accès aux appareils mobiles	Écrire	organization*		
CreateOrganization	Accorde l'autorisation de créer une nouvelle WorkMail organisation Amazon	Écrire			
CreateOutboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de créer une règle de flux de messagerie sortant qui s'applique à tous les messages envoyés à partir d'une organisation	Écrire	organization*		
CreateResource	Accorde l'autorisation de créer une nouvelle WorkMail ressource	Écrire	organization*		
CreateSmtpGateway [autorisation uniquement]	Accorde l'autorisation d'enregistrer une passerelle SMTP auprès d'une organisation WorkMail	Écrire	organization*		
CreateUser	Accorde l'autorisation de créer un utilisateur, qui peut être activée ultérieurement en appelant l' RegisterToWorkMail opération	Écrire	organization*		
DeleteAccessControlRule	Accorde l'autorisation de supprimer une règle de contrôle d'accès	Écriture	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteAlias	Accorde l'autorisation de supprimer un ou plusieurs alias spécifiés d'un ensemble d'alias pour un utilisateur donné.	Écrire	organization*		
DeleteAvailabilityConfiguration	Accorde l'autorisation de supprimer le AvailabilityConfiguration pour l' WorkMail organisation et le domaine Amazon concernés	Écrire	organization*		
DeleteEmailMonitoringConfiguration	Accorde l'autorisation de supprimer la configuration de surveillance des e-mails d'une organisation	Écrire	organization*		
DeleteGroup	Accorde l'autorisation de supprimer un groupe de WorkMail	Écrire	organization*		
DeleteIdentityCenterApplication	Accorde l'autorisation de supprimer une application Identity Center pour WorkMail	Écrire			
DeleteIdentityProviderConfiguration	Accorde l'autorisation de supprimer la configuration du fournisseur d'identité pour l'organisation	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteImpersonationRole	Accorde l'autorisation de supprimer un rôle d'usurpation d'identité pour l'organisation Amazon donnée WorkMail	Écrire	organization*		
DeleteInboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de supprimer une règle de flux de messagerie entrant pour qu'elle ne s'applique plus aux e-mails envoyés à une organisation	Écriture	organization*		
DeleteMailDomain [autorisation uniquement]	Accorde l'autorisation de supprimer un domaine de messagerie inutilisé d'une organisation	Écriture	organization*		
DeleteMailboxPermissions	Accorde l'autorisation de supprimer les autorisations accordées à un membre (utilisateur ou groupe)	Écriture	organization*		
DeleteMobileDevice [autorisation uniquement]	Accorde l'autorisation de supprimer un appareil mobile d'un utilisateur	Écrire	organization*		
DeleteMobileDeviceAccessOverride	Accorde l'autorisation de supprimer un remplacement d'accès aux appareils mobiles	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteMobileDeviceAccessRule	Accorde l'autorisation de supprimer une règle d'accès aux appareils mobiles	Écrire	organization*		
DeleteOrganization	Accorde l'autorisation de supprimer une WorkMail organisation Amazon et toutes les AWS ressources sous-jacentes gérées par Amazon dans le WorkMail cadre de l'organisation	Écrire	organization*		
DeleteOutboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de supprimer une règle de flux de messagerie sortant pour qu'elle ne s'applique plus aux e-mails envoyés à partir d'une organisation	Écrire	organization*		
DeletePersonalAccessToken	Autorise la suppression d'un jeton d'accès personnel	Écrire	organization*		
DeleteResource	Accorde l'autorisation de supprimer la ressource spécifiée	Écriture	organization*		
DeleteRetentionPolicy	Accorde l'autorisation de supprimer la politique de rétention en fonction des identifiants d'organisation et de politique fournis.	Écriture	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteSmtpGateway [autorisation uniquement]	Accorde l'autorisation de supprimer une passerelle SMTP d'une organisation	Écrire	organization*		
DeleteUser	Accorde l'autorisation de supprimer un utilisateur WorkMail de tous les systèmes suivants	Écrire	organization*		
DeliverToMailbox [autorisation uniquement]	Autorise l'envoi d'e-mails à une WorkMail organisation via l' MailManager DeliverToMailbox action SES	Écrire	organization*		
DeregisterFromWorkMail	Accorde l'autorisation de marquer un utilisateur, un groupe ou une ressource comme n'étant plus utilisé dans WorkMail	Écrire	organization*		
DeregisterMailDomain	Accorde l'autorisation d'annuler l'enregistrement d'un domaine de messagerie d'une organisation	Écrire	organization*		
DescribeEmailMonitoringConfiguration	Accorde l'autorisation de récupérer la configuration de surveillance des e-mails d'une organisation	Lecture	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeEntity	Accorde l'autorisation de lire les détails d'une entité	Lecture	organization*		
DescribeGroup	Accorde l'autorisation de lire les détails d'un groupe	List	organization*		
DescribeIdentityProviderConfiguration	Accorde l'autorisation de lire la configuration du fournisseur d'identité pour l'organisation	Lecture	organization*		
DescribeInboundDmarcSettings	Accorde l'autorisation de lire les paramètres d'une stratégie DMARC pour une organisation spécifiée	Lecture	organization*		
DescribeInboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de lire les détails d'une règle de flux de messagerie entrant configurée pour une organisation	Lecture	organization*		
DescribeMailDomains [autorisation uniquement]	Accorde l'autorisation d'affiche les détails de tous les domaines de messagerie associés à l'organisation	List	organization*		
DescribeMailboxExportJob	Accorde l'autorisation de récupérer les détails d'une tâche d'exportation de boîte aux lettres	Lecture	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeOrganization	Accorde l'autorisation de lire les détails d'une organisation	Liste	organization*		
DescribeOutboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de lire les détails d'une règle de flux de messagerie sortant configurée pour une organisation	Lecture	organization*		
DescribeResource	Accorde l'autorisation de lire les détails d'une ressource	Liste	organization*		
DescribeSmtpGateway [autorisation uniquement]	Accorde l'autorisation de lire les détails d'une passerelle SMTP enregistrée auprès d'une organisation	Lecture	organization*		
DescribeUser	Accorde l'autorisation de lire les détails d'un utilisateur	List	organization*		
DisassociateDelegateFromResource	Accorde l'autorisation de supprimer un membre de l'ensemble de délégués de la ressource	Écriture	organization*		
DisassociateMemberFromGroup	Accorde l'autorisation de supprimer un membre d'un groupe.	Écriture	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
EnableMailDomain [autorisation uniquement]	Accorde l'autorisation d'activer un domaine de messagerie dans l'organisation	Écrire	organization*		
GetAccessControlEffect	Accorde l'autorisation d'obtenir les effets des règles de contrôle d'accès telles qu'elles s'appliquent à une IPv4 adresse, à une action de protocole d'accès ou à un ID utilisateur spécifiés	Lecture	organization*		
GetDefaultRetentionPolicy	Accorde l'autorisation de récupérer la politique de rétention associée au niveau de l'organisation	Lecture	organization*		
GetImpersonationRole	Accorde l'autorisation de récupérer un rôle d'usurpation d'identité pour l'organisation Amazon donnée WorkMail	Lecture	organization*		
GetImpersonationRoleEffect	Accorde l'autorisation d'obtenir l'effet des règles associées à un rôle d'usurpation d'identité pour un utilisateur spécifique	Lecture	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetJournalingRules [autorisation uniquement]	Accorde l'autorisation de lires les adresses e-mail de journalisation et de secours configurées pour la journalisation des e-mails	Lecture	organization*		
GetMailDomain	Accorde l'autorisation de récupérer les détails d'un domaine de messagerie donné dans une organisation	Lecture	organization*		
GetMailDomainDetails [autorisation uniquement]	Accorde l'autorisation d'obtenir les détails du domaine de messagerie	Lecture	organization*		
GetMailboxDetails	Accorde l'autorisation de lire les détails de la boîte aux lettres de l'utilisateur	Lecture	organization*		
GetMobileDeviceAccessEffect	Accorde l'autorisation de simuler l'effet des règles d'accès aux appareils mobiles pour les attributs donnés d'un exemple d'événement d'accès	Lecture	organization*		
GetMobileDeviceAccessOverride	Accorde l'autorisation de récupérer un remplacement d'accès aux appareils mobiles	Lecture	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetMobileDeviceDetails [autorisation uniquement]	Accorde l'autorisation d'obtenir les détails de l'appareil mobile	Lecture	organization*		
GetMobileDevicesForUser [autorisation uniquement]	Accorde l'autorisation d'obtenir la liste des appareils mobiles associés à l'utilisateur	Lecture	organization*		
GetMobilePolicyDetails [autorisation uniquement]	Accorde l'autorisation d'obtenir les détails de la politique d'appareil mobile associée à l'organisation	Lecture	organization*		
GetPersonalAccessTokenMetadata	Accorde l'autorisation de lire les métadonnées d'un jeton d'accès personnel	Lecture	organization*		
ListAccessControlRules	Accorde l'autorisation de répertorier les règles de contrôle d'accès	Lecture	organization*		
ListAliases	Accorde l'autorisation de répertorier les alias associés à une entité donnée	List	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAvailabilityConfigurations	Octroie l'autorisation de répertorier tous AvailabilityConfiguration les éléments pour l' WorkMail organisation Amazon donnée	Lecture	organization*		
ListGroupMembers	Accorde l'autorisation de lire une vue d'ensemble des membres d'un groupe. Les utilisateurs et les groupes peuvent être membres d'un groupe	Liste	organization*		
ListGroups	Accorde l'autorisation de répertorier des récapitulatifs des groupes de l'organisation.	List	organization*		
ListGroupsForEntity	Accorde l'autorisation de répertorier les groupes auxquels une entité appartient	List	organization*		
ListImpersonationRoles	Accorde l'autorisation de répertorier les rôles d'usurpation d'identité pour l'organisation Amazon donnée WorkMail	List	organization*		
ListInboundMailFlowRules [autorisation uniquement]	Accorde l'autorisation de répertorier les règles de flux de messagerie entrant configurées pour une organisation	List	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListMailDomains	Accorde l'autorisation de répertorier les domaines de messagerie d'une organisation donnée	List	organization*		
ListMailboxExportJobs	Accorde l'autorisation de répertorier les tâches d'exportation de boîtes aux lettres	Liste	organization*		
ListMailboxPermissions	Accorde l'autorisation de répertorier les autorisations de boîte aux lettres associées à une boîte aux lettres utilisateur, groupe ou ressource.	List	organization*		
ListMobileDeviceAccessOverrides	Accorde l'autorisation de répertorier les remplacements d'accès aux appareils mobiles	Lecture	organization*		
ListMobileDeviceAccessRules	Accorde l'autorisation de répertorier les règles d'accès aux appareils mobiles	Lecture	organization*		
ListOrganizations	Accorde l'autorisation de répertorier les organisations non supprimées	Liste			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListOutboundMailFlowRules [autorisation uniquement]	Accorde l'autorisation de répertorier les règles de flux de messagerie sortant configurées pour une organisation	List	organization*		
ListPersonalAccessTokens	Accorde l'autorisation de répertorier les métadonnées pour les jetons d'accès personnels	List	organization*		
ListResourceDelegates	Accorde l'autorisation de répertorier les délégués associés à une ressource.	Liste	organization*		
ListResources	Accorde l'autorisation de répertorier les ressources de l'organisation	Liste	organization*		
ListSmtpGateways [autorisation uniquement]	Accorde l'autorisation de répertorier les passerelles SMTP enregistrées dans l'organisation	List	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises appliquées à une ressource d' WorkMail organisation Amazon	List	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListUsers	Accorde l'autorisation de répertorier les utilisateurs de l'organisation	Liste	organization*		
PutAccessControlRule	Accorde l'autorisation d'ajouter une nouvelle règle de contrôle d'accès	Écrire	organization*		
PutEmailMonitoringConfiguration	Accorde l'autorisation d'ajouter ou de mettre à jour la configuration de surveillance des e-mails d'une organisation	Écrire	organization*		
PutIdentityProviderConfiguration	Accorde l'autorisation d'ajouter ou de mettre à jour la configuration du fournisseur d'identité pour l'organisation	Écrire	organization*		
PutInboundDmarcSettings	Accorde l'autorisation d'activer ou de désactiver une stratégie DMARC pour une organisation donnée	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutMailboxPermissions	Accorde l'autorisation de définir des autorisations pour un utilisateur, un groupe ou une ressource, en remplaçant toutes les autorisations existantes	Écrire	organization*		
PutMobileDeviceAccessOverride	Accorde l'autorisation d'aouter ou de mettre à jour un remplacement d'accès aux appareils mobiles	Écrire	organization*		
PutRetentionPolicy	Accorde l'autorisation d'ajouter ou de mettre à jour la politique de rétention	Écrire	organization*		
RegisterMailDomain	Accorde l'autorisation d'enregistrer un nouveau domaine de messagerie dans une organisation	Écrire	organization*		
RegisterToWorkMail	Accorde l'autorisation d'enregistrer un utilisateur, un groupe ou une ressource existant ou désactivé à utiliser en associant une boîte aux lettres et des fonctionnalités de calendrier	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ResetPassword	Accorde l'autorisation à l'administrateur de réinitialiser le mot de passe d'un utilisateur	Écriture	organization*		
SearchMembers [autorisation uniquement]	Accorde l'autorisation d'effectuer une recherche par préfixe pour trouver un utilisateur spécifique dans un groupe de messagerie	Lecture	organization*		
SetDefaultMailDomain [autorisation uniquement]	Accorde l'autorisation de définir le domaine de messagerie par défaut pour l'organisation	Écriture	organization*		
SetJournalingRules [autorisation uniquement]	Accorde l'autorisation de définir les adresses e-mail de journalisation et de secours pour la journalisation des e-mails	Écriture	organization*		
SetMobilePolicyDetails [autorisation uniquement]	Accorde l'autorisation de définir les détails d'une politique mobile associée à l'organisation	Écriture	organization*		
StartMailboxExportJob	Accorde l'autorisation de démarrer une nouvelle tâche d'exportation de boîtes aux lettres	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
TagResource	Accorde l'autorisation de baliser la ressource d' WorkMail organisation Amazon spécifiée	Identification	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestAvailabilityConfiguration	Accorde l'autorisation d'effectuer un test sur un fournisseur de disponibilité pour s'assurer que l'accès est autorisé	Lecture	organization*		
TestInboundMailFlowRules [autorisation uniquement]	Accorde l'autorisation de tester les règles entrantes qui s'appliqueront à un e-mail avec un expéditeur et un destinataire donnés	Écriture	organization*		
TestOutboundMailFlowRules [autorisation uniquement]	Accorde l'autorisation de tester les règles sortantes qui s'appliqueront à un e-mail avec un expéditeur et un destinataire donnés	Écrire	organization*		
UntagResource	Accorde l'autorisation de supprimer le balisage de la ressource d' WorkMail organisation Amazon spécifiée	Identification	organization*		
				aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateAvailabilityConfiguration	Autorise la mise à jour d'une WorkMail organisation et d'un domaine Amazon existants AvailabilityConfiguration	Écrire	organization*		
UpdateDefaultMailDomain	Accorde l'autorisation de mettre à jour quel domaine est le domaine par défaut d'une organisation.	Écrire	organization*		
UpdateGroup	Accorde l'autorisation de mettre à jour les détails d'un groupe	Écrire	organization*		
UpdateImpersonationRole	Accorde l'autorisation de mettre à jour un rôle d'usurpation d'identité existant pour l'organisation Amazon donnée WorkMail	Écrire	organization*		
UpdateInboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de mettre à jour les détails d'une règle de flux de messagerie entrant qui s'applique à tous les messages envoyés à une organisation	Écriture	organization*		
UpdateMailboxQuota	Accorde l'autorisation de mettre à jour la taille maximale (en Mo) de la boîte aux lettres de l'utilisateur.	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateMobileDeviceAccessRule	Accorde l'autorisation de mettre à jour une règle d'accès aux appareils mobiles	Écrire	organization*		
UpdateOutboundMailFlowRule [autorisation uniquement]	Accorde l'autorisation de mettre à jour les détails d'une règle de flux de messagerie sortant qui s'applique à tous les messages envoyés à partir d'une organisation	Écriture	organization*		
UpdatePrimaryEmailAddress	Accorde l'autorisation de mettre à jour l'e-mail principal d'un utilisateur, d'un groupe ou d'une ressource.	Écriture	organization*		
UpdateResource	Accorde l'autorisation de mettre à jour des détails de la ressource.	Écriture	organization*		
UpdateSmtpGateway [autorisation uniquement]	Accorde l'autorisation de mettre à jour les détails d'une passerelle SMTP existante enregistrée auprès d'une organisation	Écrire	organization*		
UpdateUser	Accorde l'autorisation de mettre à jour les détails d'un utilisateur	Écrire	organization*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
WipeMobileDevice [autorisation uniquement]	Accorde l'autorisation d'effacer à distance l'appareil mobile associé au compte d'un utilisateur	Écrire	organization*		

Types de ressources définis par Amazon WorkMail

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
organization	`arn:${Partition}:workmail:${Region}:${Account}:organization/${ResourceId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon WorkMail

Amazon WorkMail définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur de la balise transmises dans la demande	String
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des paires clé-valeur d'identification attachées à la ressource	String
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
workmail:ImpersonationRoleId	Filtre l'accès en fonction de ImpersonationRoleId ce qui est transmis dans la demande	String

Actions, ressources et clés de condition pour Amazon WorkMail Message Flow

Amazon WorkMail Message Flow (préfixe de service :`workmailmessageflow`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkMail Message Flow
- Types de ressources définis par Amazon WorkMail Message Flow
- Clés de condition pour Amazon WorkMail Message Flow

Actions définies par Amazon WorkMail Message Flow

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la

colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetRawMessageContent	Accorde l'autorisation de lire le contenu des e-mails avec l'ID de message spécifié	Lecture	RawMessage*		
PutRawMessageContent	Accorde l'autorisation de mettre à jour le contenu des e-mails avec l'ID de message spécifié	Écrire	RawMessage*		

Types de ressources définis par Amazon WorkMail Message Flow

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
RawMessage	`arn:${Partition}:workmailmessageflow:${Region}:${Account}:message/${OrganizationId}/${Context}/${MessageId}`	

Clés de condition pour Amazon WorkMail Message Flow

WorkMail Message Flow ne possède aucune clé de contexte spécifique au service pouvant être utilisée dans l'`Condition`élément des déclarations de politique. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour Amazon WorkSpaces

Amazon WorkSpaces (préfixe de service :`workspaces`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkSpaces
- Types de ressources définis par Amazon WorkSpaces
- Clés de condition pour Amazon WorkSpaces

Actions définies par Amazon WorkSpaces

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez

généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AcceptAccountLinkInvitation	Accorde l'autorisation d'accepter des invitations provenant d'autres AWS comptes pour partager la même configuration pour WorkSpaces BYOL	Écrire			
AssociateConnectionAlias	Accorde l'autorisation d'associer des alias de connexion à des répertoires.	Écriture	connectionalias*		
			directoryid*		
AssociateIpGroups	Accorde l'autorisation d'associer des groupes de contrôle d'accès IP à des répertoires.	Écrire	directoryid*		
			workspaceipgroup*		
AssociateWorkspaceApplication	Accorde l'autorisation d'associer une application d'espace de travail à WorkSpace	Écrire	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AuthorizeIpRules	Accorde l'autorisation d'ajouter des règles aux groupes de contrôle d'accès IP.	Écrire	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
CopyWorkspaceImage	Autorise la copie d'une WorkSpace image	Écrire	workspaceimage*		workspaces:DescribeWorkspaceImages
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountLinkInvitation	Accorde l'autorisation d'inviter d'autres AWS comptes à partager la même configuration pour WorkSpaces BYOL	Écrire			
CreateConnectClientAddIn	Accorde l'autorisation de créer une extension client Amazon Connect dans un répertoire	Écrire	directoryid*		
CreateConnectionAlias	Accorde l'autorisation de créer des alias de connexion à utiliser avec la redirection entre régions.	Écriture		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateIpGroup	Accorde l'autorisation de créer des groupes de contrôle d'accès IP.	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRootClientCertificate [autorisation uniquement]	Accorde l'autorisation de créer un certificat client racine	Écrire	certificateid*		
CreateStandbyWorkspaces	Accorde l'autorisation de créer un ou plusieurs Standby WorkSpaces	Écrire	directoryid*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Accorde l'autorisation de créer des balises pour les WorkSpaces ressources	Identification		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateUpdatedWorkspaceImage	Accorde l'autorisation de créer une WorkSpace image mise à jour	Écrire	workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceBundle	Accorde l'autorisation de créer un WorkSpace bundle	Écrire	workspacebundle*		workspaces:CreateTags
			workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceImage	Accorde l'autorisation de créer une nouvelle WorkSpace image	Écrire	workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateWorkspaces	Accorde l'autorisation d'en créer un ou plusieurs WorkSpaces	Écrire	directoryid*	aws:ResourceTag/${TagKey}	
			workspacebundle*	aws:ResourceTag/${TagKey}	
			workspaceid*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspacesPool	Accorde l'autorisation de créer un WorkSpaces pool	Écrire	directoryid*		
			workspacebundle*		
			workspacespoolid*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountLinkInvitation	Accorde l'autorisation de supprimer des invitations à d'autres AWS comptes afin de partager la même configuration pour WorkSpaces BYOL	Écrire			
DeleteClientBranding	Accorde l'autorisation de supprimer les données de marque du AWS WorkSpaces client dans un répertoire	Écrire	directoryid*		
DeleteConnectClientAddIn	Accorde l'autorisation de supprimer une extension client Amazon Connect configurée dans un répertoire	Écrire	directoryid*		
DeleteConnectionAlias	Accorde l'autorisation de supprimer des alias de connexion.	Écriture	connectionalias*		
DeleteIpGroup	Accorde l'autorisation de supprimer des groupes de contrôle d'accès IP.	Écrire	workspaceipgroup*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteRootClientCertificate [autorisation uniquement]	Accorde l'autorisation de supprimer le certificat client racine	Écrire	certificateid*		
DeleteTags	Accorde l'autorisation de supprimer des balises des WorkSpaces ressources	Identification		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWorkspaceBundle	Accorde l'autorisation de supprimer des WorkSpace bundles	Écrire	workspacebundle*		
DeleteWorkspaceImage	Autorise la suppression d' WorkSpace images	Écrire	workspaceimage*		
DeployWorkspaceApplications	Autorise le déploiement de toutes les applications d'espace de travail en attente sur un WorkSpace	Écrire	workspaceid*		
				aws:ResourceTag/${TagKey}	
DeregisterWorkspaceDirectory	Accorde l'autorisation de désenregistrer les annuaires pour qu'ils ne soient plus utilisés par Amazon WorkSpaces	Écrire	directoryid*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeAccount	Accorde l'autorisation de récupérer la configuration de Bring Your Own License (BYOL) pour les comptes WorkSpaces	Lecture			
DescribeAccountModifications	Accorde l'autorisation de récupérer les modifications apportées à la configuration de Bring Your Own License (BYOL) pour les comptes WorkSpaces	Lecture			
DescribeApplicationAssociations	Accorde l'autorisation de récupérer des informations sur les ressources associées à une WorkSpace application	List	workspaceapplication*		
				aws:ResourceTag/${TagKey}	
DescribeApplications	Donne l'autorisation d'obtenir des informations sur WorkSpace les demandes	List			
DescribeBundleAssociations	Accorde l'autorisation de récupérer des informations sur les ressources associées à un WorkSpace bundle	List	workspacebundle*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeClientBranding	Accorde l'autorisation de récupérer les données de marque du AWS WorkSpaces client dans un annuaire	Lecture	directory id*		
DescribeClientProperties	Accorde l'autorisation de récupérer des informations sur WorkSpaces les clients	List	directory id*		
DescribeConnectClientAddIns	Accorde l'autorisation de récupérer une liste des extensions client Amazon Connect qui ont été créées	List	directory id*		
DescribeConnectionAliasPermissions	Accorde l'autorisation de récupérer les autorisations que les propriétaires d'alias de connexion ont accordées à d'autres AWS comptes pour les alias de connexion	Lecture	connectionalias*		
DescribeConnectionAliases	Accorde l'autorisation de récupérer une liste qui décrit les alias de connexion utilisés pour la redirection entre régions.	Lecture			
DescribeConsent [autorisation uniquement]	Accorde l'autorisation de récupérer des informations sur l'accord de consentement conformément aux exigences minimales du BYOL	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeCustomWorkspaceImageImport	Accorde l'autorisation de récupérer des informations sur la tâche d'importation d'images WorkSpace BYOL	Lecture			
DescribeImageAssociations	Accorde l'autorisation de récupérer des informations sur les ressources associées à une WorkSpace image	List	workspaceimage*		
				aws:ResourceTag/${TagKey}	
DescribeIpGroups	Accorde l'autorisation de récupérer des informations sur les groupes de contrôle d'accès IP.	Lecture	workspaceipgroup*		
DescribeTags	Accorde l'autorisation de décrire les balises des WorkSpaces ressources	Lecture			
DescribeWorkspaceAssociations	Octroie l'autorisation de récupérer des informations sur les ressources associées à un WorkSpace	List	workspaceid*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceBundles	Accorde l'autorisation d'obtenir des informations sur les WorkSpace offres groupées	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWorkspaceDirectories	Accorde l'autorisation de récupérer des informations sur les annuaires enregistrés auprès de WorkSpaces	Lecture			
DescribeWorkspaceImagePermissions	Accorde l'autorisation de récupérer des informations sur les autorisations relatives aux WorkSpace images	Lecture	workspaceimage*		
DescribeWorkspaceImages	Accorde l'autorisation de récupérer des informations sur les WorkSpace images	List			
DescribeWorkspaceSnapshots	Accorde l'autorisation de récupérer des informations sur les WorkSpace instantanés	List	workspaceid*		
DescribeWorkspaces	Accorde l'autorisation d'obtenir des informations sur WorkSpaces	List			
DescribeWorkspacesConnectionStatus	Accorde l'autorisation d'obtenir l'état de connexion de WorkSpaces	Lecture			
DescribeWorkspacesPoolSessions	Accorde l'autorisation de récupérer des informations sur les sessions d'un WorkSpaces pool	List	workspacespoolid*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DescribeWorkspacesPools	Accorde l'autorisation de récupérer des informations sur les WorkSpaces pools	List			
DirectoryAccessManagement [autorisation uniquement]	Accorde l'autorisation d'effectuer des actions de gestion d'annuaires lors de la gestion et du provisionnement des espaces de travail	List	directoryid*		
DisassociateConnectionAlias	Accorde l'autorisation de dissocier des alias de connexion des répertoires.	Écriture	connectionalias*		
DisassociateIpGroups	Accorde l'autorisation de dissocier des groupes de contrôle d'accès IP des répertoires.	Écrire	directoryid*		
			workspaceipgroup*		
DisassociateWorkspaceApplication	Accorde l'autorisation de dissocier une application d'espace de travail d'un WorkSpace	Écrire	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetAccountLink	Accorde l'autorisation de récupérer un lien avec un autre AWS compte pour partager la configuration pour WorkSpaces BYOL	Lecture			
ImportClientBranding	Autorise l'importation des données de marque du AWS WorkSpaces client dans un annuaire	Écrire	directoryid*		
ImportCustomWorkspaceImage	Autorise l'importation d'images Bring Your Own License (BYOL) sur Amazon WorkSpaces	Écrire			
ImportWorkspaceImage	Autorise l'importation d'images Bring Your Own License (BYOL) sur Amazon WorkSpaces	Écrire			ec2:DescribeImages ec2:ModifyImageAttribute
ListAccountLinks	Accorde l'autorisation de récupérer des liens avec le ou les AWS comptes qui partagent votre configuration pour WorkSpaces BYOL	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListAvailableManagementCidrRanges	Permet de répertorier les plages CIDR disponibles pour activer la licence BYOL (Bring Your Own License) pour les comptes WorkSpaces	List			
MigrateWorkspace	Accorde l'autorisation de migrer WorkSpaces	Écrire	workspacebundle*		
			workspaceid*		
ModifyAccount	Accorde l'autorisation de modifier la configuration de Bring Your Own License (BYOL) pour les comptes WorkSpaces	Écrire			
ModifyCertificateBasedAuthProperties	Accorde l'autorisation de modifier les propriétés d'autorisation basées sur les certificats d'un répertoire	Écrire	directoryid*		
ModifyClientProperties	Accorde l'autorisation de modifier les propriétés des WorkSpaces clients	Écrire	directoryid*		
ModifyEndpointEncryptionMode	Accorde l'autorisation de configurer le répertoire spécifié entre le mode TLS standard et le mode validé FIPS 140-2	Écrire	directoryid*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifySamlProperties	Accorde l'autorisation de modifier les propriétés SAML d'un répertoire	Écrire	directory id*		
ModifySelfservicePermissions	Autorise vos utilisateurs à modifier les fonctionnalités WorkSpace de gestion en libre-service	Gestion des autorisations	directory id*		
ModifyStreamingProperties	Accorde l'autorisation de modifier les propriétés de diffusion	Écrire	directory id*		
ModifyWorkspaceAccessProperties	Accorde l'autorisation de spécifier les appareils et systèmes d'exploitation que les utilisateurs peuvent utiliser pour accéder à leurs WorkSpaces	Écrire	directory id*		
ModifyWorkspaceCreationProperties	Accorde l'autorisation de modifier les propriétés par défaut utilisées pour créer WorkSpaces	Écrire	directory id*		
ModifyWorkspaceProperties	Accorde l'autorisation de modifier les WorkSpace propriétés, y compris le mode d'exécution et la AutoStop période	Écrire	workspace id*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ModifyWorkspaceState	Accorde l'autorisation de modifier l'état de WorkSpaces	Écrire	workspace id*		
RebootWorkspaces	Accorde l'autorisation de redémarrer WorkSpaces	Écrire	workspace id*		
RebuildWorkspaces	Donne l'autorisation de reconstruire WorkSpaces	Écrire	workspace id*		
RegisterWorkspaceDirectory	Accorde l'autorisation d'enregistrer des annuaires destinés à être utilisés par Amazon WorkSpaces	Écrire	directory id*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RejectAccountLinkInvitation	Accorde l'autorisation de rejeter les invitations d'autres AWS comptes à partager la même configuration pour WorkSpaces BYOL	Écrire			
RestoreWorkspace	Accorde l'autorisation de restauration WorkSpaces	Écrire	workspace id*		
RevokeIpRules	Accorde l'autorisation de supprimer des règles des groupes de contrôle d'accès IP.	Écrire	workspace ipgroup*		workspaces:UpdateRulesOfIpGroup

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
StartWorkspaces	Accorde l'autorisation de démarrer AutoStop WorkSpaces	Écrire	workspaceid*		
StartWorkspacesPool	Accorde l'autorisation de démarrer un WorkSpaces pool	Écrire	workspacespoolid*		
StopWorkspaces	Donne l'autorisation d'arrêter AutoStop WorkSpaces	Écrire	workspaceid*		
StopWorkspacesPool	Autorise l'arrêt d'un WorkSpaces pool	Écrire	workspacespoolid*		
Stream	Accorde l'autorisation aux utilisateurs fédérés de se connecter à l'aide de leurs informations d'identification existantes et de diffuser leur espace de travail	Écrire	directoryid*		
				workspaces:userId	
TerminateWorkspaces	Accorde l'autorisation de résilier WorkSpaces	Écrire	workspaceid*		
TerminateWorkspacesPool	Accorde l'autorisation de mettre fin à un WorkSpaces pool	Écrire	workspacespoolid*		
TerminateWorkspacesPoolSession	Accorde l'autorisation de mettre fin à une session de WorkSpaces pool	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateConnectClientAddIn	Accorde l'autorisation de mettre à jour une extension client Amazon Connect. Utilisez cette action pour mettre à jour le nom et l'URL du point de terminaison d'une extension client Amazon Connect	Écrire	directoryid*		
UpdateConnectionAliasPermission	Accorde l'autorisation de partager ou d'annuler le partage des alias de connexion avec d'autres comptes.	Gestion des autorisations	connectionalias*		
UpdateConsent [autorisation uniquement]	Autorise la mise à jour de l'accord de consentement conformément aux exigences minimales du BYOL	Écrire			
UpdateRootClientCertificate [autorisation uniquement]	Autorise la mise à jour d'un certificat client racine	Écrire	certificateid*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateRulesOfIpGroup	Accorde l'autorisation de remplacer des règles des groupes de contrôle d'accès IP.	Écrire	workspaceipgroup*		workspaces:AuthorizeIpRules workspaces:RevokeIpRules
UpdateWorkspaceBundle	Accorde l'autorisation de mettre à jour les WorkSpace images utilisées dans les WorkSpace bundles	Écrire	workspacebundle* workspaceimage*		
UpdateWorkspaceImagePermission	Accorde l'autorisation de partager ou d'annuler le partage d' WorkSpace images avec d'autres comptes en spécifiant si les autres comptes sont autorisés à copier l'image	Gestion des autorisations	workspaceimage*		
UpdateWorkspacesPool	Autorise la mise à jour du WorkSpaces pool	Écrire	workspacespoolid*		

Types de ressources définis par Amazon WorkSpaces

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont

affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
certificateid	arn:${Partition}:workspaces:${Region}:${Account}:workspacecertificate/${CertificateId}	
directoryid	arn:${Partition}:workspaces:${Region}:${Account}:directory/${DirectoryId}	aws:ResourceTag/${TagKey}
workspacebundle	arn:${Partition}:workspaces:${Region}:${Account}:workspacebundle/${BundleId}	aws:ResourceTag/${TagKey}
workspaceid	arn:${Partition}:workspaces:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
workspaceimage	arn:${Partition}:workspaces:${Region}:${Account}:workspaceimage/${ImageId}	aws:ResourceTag/${TagKey}
workspaceipgroup	arn:${Partition}:workspaces:${Region}:${Account}:workspaceipgroup/${GroupId}	aws:ResourceTag/${TagKey}
workspacespoolid	arn:${Partition}:workspaces:${Region}:${Account}:workspacespool/${PoolId}	aws:ResourceTag/${TagKey}
connectionalias	arn:${Partition}:workspaces:${Region}:${Account}:connectionalias/${ConnectionAliasId}	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
workspace application	`arn:${Partition}:workspaces:${Region}:${Account}:workspaceapplication/${WorkSpaceApplicationId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon WorkSpaces

Amazon WorkSpaces définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString
workspaces:userId	Filtre l'accès en fonction de l'ID de l'utilisateur Workspaces	String

Actions, ressources et clés de condition pour Amazon WorkSpaces Application Manager

Amazon WorkSpaces Application Manager (préfixe de service :`wam`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkSpaces Application Manager
- Types de ressources définis par Amazon WorkSpaces Application Manager
- Clés de condition pour Amazon WorkSpaces Application Manager

Actions définies par Amazon WorkSpaces Application Manager

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette

action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AuthenticatePackager [autorisation uniquement]	Permet à l'instance d'empaquetage Amazon WAM d'accéder à votre catalogue de packages d'application.	Écrire			

Types de ressources définis par Amazon WorkSpaces Application Manager

Amazon WorkSpaces Application Manager ne prend pas en charge la spécification d'un ARN de ressource dans l'`Resource`élément d'une déclaration de politique IAM. Pour autoriser l'accès à Amazon WorkSpaces Application Manager, `"Resource": "*"` spécifiez-le dans votre politique.

Clés de condition pour Amazon WorkSpaces Application Manager

WAM ne comporte aucune clé de contexte spécifique au service pouvant être utilisée dans l'élément `Condition` des déclarations de stratégie. Pour obtenir la liste des clés de contexte globales disponibles pour tous les services, consultez la section Clés de contexte de condition AWS globales.

Actions, ressources et clés de condition pour les instances AWS WorkSpaces gérées

AWS WorkSpaces Les instances gérées (préfixe de service :`workspaces-instances`) fournissent les ressources, actions et clés de contexte de condition spécifiques au service suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par les instances AWS WorkSpaces gérées
- Types de ressources définis par les instances AWS WorkSpaces gérées
- Clés de condition pour les instances AWS WorkSpaces gérées

Actions définies par les instances AWS WorkSpaces gérées

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois,

dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateVolume	Accorde l'autorisation d'associer un volume géré de l'espace de travail à une instance gérée de l'espace de travail dans votre compte	Écrire	WorkspaceInstanceId*		ec2:AttachVolume ec2:DescribeVolumes
CreateVolume	Autorise la création d'un volume géré par un espace de travail dans votre compte	Écrire			ec2:CreateVolume
CreateWorkspaceInstance	Accorde l'autorisation de créer une instance gérée de l'espace de travail dans votre compte	Écrire		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:RunInstances
DeleteVolume	Autorise la suppression d'un volume géré par l'espace de travail dans votre compte	Écrire	VolumeId*		ec2:DeleteVolume ec2:DescribeVolumes
DeleteWorkspaceInstance	Accorde l'autorisation de supprimer une instance gérée de l'espace de travail dans votre compte	Écrire	WorkspaceInstanceId*		ec2:TerminateInstances
DisassociateVolume	Accorde l'autorisation de dissocier un volume géré par un espace de travail d'une	Écrire	WorkspaceInstanceId*		ec2:DescribeVolumes

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	instance gérée par un espace de travail dans votre compte				ec2:DetachVolume
GetWorkspaceInstance	Accorde l'autorisation d'obtenir les détails d'une instance gérée d'espace de travail spécifique dans votre compte	Lecture	WorkspaceInstanceId*		
ListInstanceTypes	Accorde l'autorisation de répertorier tous les types d'instances pris en charge	List			
ListRegions	Donne l'autorisation de répertorier toutes les AWS régions prises en charge	List			
ListTagsForResource	Accorde l'autorisation de répertorier les balises utilisateur pour les ressources de votre compte	List	WorkspaceInstanceId*		
ListWorkspaceInstances	Accorde l'autorisation de répertorier les instances gérées par l'espace de travail dans votre compte	List			
TagResource	Autorise l'ajout de balises utilisateur aux ressources de votre compte	Identification	WorkspaceInstanceId*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Accorde l'autorisation de supprimer les tags utilisateur des ressources de votre compte	Identification	WorkspaceInstanceId*		
				aws:TagKeys	

Types de ressources définis par les instances AWS WorkSpaces gérées

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
WorkspaceInstanceId	`arn:${Partition}:workspaces-instances:${Region}:${Account}:workspaceinstance/${WorkspaceInstanceId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
VolumeId	`arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}`	aws:ResourceTag/${TagKey}

Clés de condition pour les instances AWS WorkSpaces gérées

AWS WorkSpaces Managed Instances définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser (préfixe de service :`workspaces-web`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkSpaces Secure Browser
- Types de ressources définis par Amazon WorkSpaces Secure Browser
- Clés de condition pour Amazon WorkSpaces Secure Browser

Actions définies par Amazon WorkSpaces Secure Browser

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate BrowserSettings	Accorde l'autorisation d'associer les paramètres du navigateur à des portails web	Écrire	browserSettings*		
			portal*		
Associate DataProtectionSettings	Accorde l'autorisation d'associer les paramètres de protection des données aux portails Web	Écrire	dataProtectionSettings*		
			portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
Associate IpAccessSettings	Accorde l'autorisation d'associer des paramètres d'accès IP à des portails Web.	Écrire	ipAccessSettings*		
			portal*		
Associate NetworkSettings	Accorde l'autorisation d'associer des paramètres réseau à des portails web	Écrire	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
			portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
AssociateSessionLogger	Autorise l'association d'un enregistreur de session à des portails Web	Écrire	portal*		
			sessionLogger*		
AssociateTrustStore	Accorde l'autorisation d'associer des magasins d'approbations à des portails web	Écrire	portal*		
			trustStore*		
AssociateUserAccessLoggingSettings	Accorde l'autorisation d'associer des paramètres de journalisation d'accès utilisateur à des portails web	Écrire	portal*		kinesis:PutRecord kinesis:PutRecords
			userAccessLoggingSettings*		
AssociateUserSettings	Accorde l'autorisation d'associer des paramètres utilisateur à des portails web	Écrire	portal*		
			userSettings*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateBrowserSettings	Accorde l'autorisation de créer des paramètres de navigateur	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey workspaces-web:TagResource
CreateDataProtectionSettings	Accorde l'autorisation de créer des paramètres de protection des données	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateIdentityProvider	Accorde l'autorisation de créer des fournisseurs d'identité	Écrire	identityProvider* portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIpAccessSettings	Accorde l'autorisation de créer des paramètres d'accès IP.	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateNetworkSettings	Accorde l'autorisation de créer des paramètres réseau	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole workspaces-web:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreatePortal	Accorde l'autorisation de créer des portails web	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey workspaces-web:TagResource
CreateSessionLogger	Accorde l'autorisation de créer un enregistreur de session	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	s3:PutObject workspaces-web:TagResource

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateTrustStore	Accorde l'autorisation de créer des magasins d'approbations	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateUserAccessLoggingSettings	Accorde l'autorisation de créer des paramètres de journalisation d'accès utilisateur	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateUserSettings	Accorde l'autorisation de créer des paramètres utilisateur	Écrire		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
DeleteBrowserSettings	Accorde l'autorisation de supprimer des paramètres de navigateur	Écrire	browserSettings*		
DeleteDataProtectionSettings	Autorise la suppression des paramètres de protection des données	Écrire	dataProtectionSettings*		
DeleteIdentityProvider	Accorde l'autorisation de supprimer des fournisseurs d'identité	Écrire	identityProvider*		
			portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DeleteIpAccessSettings	Accorde l'autorisation de supprimer des paramètres d'accès IP.	Écrire	ipAccessSettings*		
DeleteNetworkSettings	Accorde l'autorisation de supprimer des paramètres réseau	Écrire	networkSettings*		
DeletePortal	Accorde l'autorisation de supprimer des portails web	Écrire	portal*		
DeleteSessionLogger	Autorise la suppression de l'enregistreur de session	Écrire	sessionLogger*		
DeleteTrustStore	Accorde l'autorisation de supprimer des magasins d'approbations	Écrire	trustStore*		
DeleteUserAccessLoggingSettings	Accorde l'autorisation de supprimer les paramètres de journalisation d'accès utilisateur	Écrire	userAccessLoggingSettings*		
DeleteUserSettings	Accorde l'autorisation de supprimer des paramètres utilisateur	Écrire	userSettings*		
DisassociateBrowserSettings	Accorde l'autorisation de dissocier les paramètres de navigateur des portails web	Écrire	portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
DisassociateDataProtectionSettings	Autorise à dissocier la journalisation de la protection des données des portails Web	Écrire	portal*		
DisassociateIpAccessSettings	Accorde l'autorisation de dissocier la journalisation d'accès IP des portails Web.	Écrire	portal*		
DisassociateNetworkSettings	Accorde l'autorisation de dissocier les paramètres réseau des portails web	Écrire	portal*		
DisassociateSessionLogger	Accorde l'autorisation de dissocier l'enregistreur de session des portails Web	Écrire	portal*		
DisassociateTrustStore	Accorde l'autorisation de dissocier les magasins d'approbations des portails web	Écrire	portal*		
DisassociateUserAccessLoggingSettings	Accorde l'autorisation de dissocier les paramètres de journalisation d'accès utilisateur des portails web	Écrire	portal*		
DisassociateUserSettings	Accorde l'autorisation de dissocier les paramètres utilisateur des portails web	Écrire	portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ExpireSession	Accorde l'autorisation d'expirer une session à partir d'un portail spécifique	Écrire	portal*		
GetBrowserSettings	Accorde l'autorisation d'obtenir des détails sur les paramètres de navigateur	Lecture	browserSettings*		
GetDataProtectionSettings	Accorde l'autorisation d'obtenir des détails sur les paramètres de protection des données	Lecture	dataProtectionSettings*		
GetIdentityProvider	Accorde l'autorisation d'obtenir des détails sur les fournisseurs d'identité	Lecture	identityProvider*		
GetIpAccessSettings	Accorde l'autorisation d'obtenir des détails sur des paramètres d'accès IP.	Lecture	ipAccessSettings*		
GetNetworkSettings	Accorde l'autorisation d'obtenir des détails sur les paramètres réseau	Lecture	networkSettings*		
GetPortal	Accorde l'autorisation d'obtenir des détails sur des portails web	Lecture	portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetPortalServiceProviderMetadata	Accorde l'autorisation d'obtenir des informations de métadonnées de fournisseur de services pour les portails web	Lecture	portal*		
GetSession	Accorde l'autorisation d'obtenir des informations sur une session particulière pour un portail	Lecture	portal*		
GetSessionLogger	Accorde l'autorisation d'obtenir des détails sur l'enregistreur de session	Lecture	sessionLogger*		
GetTrustStore	Accorde l'autorisation d'obtenir des détails sur les magasins d'approbations	Lecture	trustStore*		
GetTrustStoreCertificate	Accorde l'autorisation d'obtenir des certificats à partir des magasins d'approbations	Lecture	trustStore*		
GetUserAccessLoggingSettings	Accorde l'autorisation d'obtenir des détails sur les paramètres de journalisation d’accès utilisateur	Lecture	userAccessLoggingSettings*		
GetUserSettings	Accorde l'autorisation d'obtenir des détails sur les paramètres utilisateur	Lecture	userSettings*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListBrowserSettings	Accorde l'autorisation de répertorier les paramètres de navigateur	Lecture			
ListDataProtectionSettings	Accorde l'autorisation de répertorier les paramètres de protection des données	Lecture			
ListIdentityProviders	Accorde l'autorisation de répertorier les fournisseurs d'identité	Lecture	identityProvider*		
ListIpAccessSettings	Accorde l'autorisation de répertorier des paramètres d'accès IP.	Lecture			
ListNetworkSettings	Accorde l'autorisation de répertorier les paramètres réseau	Lecture			
ListPortals	Accorde l'autorisation de répertorier les portails web	Lecture			
ListSessionLoggers	Accorde l'autorisation de répertorier les enregistreurs de session	Lecture			
ListSessions	Accorde l'autorisation de répertorier les sessions d'un portail à l'aide de filtres facultatifs	Lecture	portal*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les identifications d'une ressource	Lecture			
ListTrustStoreCertificates	Accorde l'autorisation de répertorier les certificats dans un magasin d'approbations	Lecture			
ListTrustStores	Accorde l'autorisation de répertorier les magasins d'approbations	Lecture			
ListUserAccessLoggingSettings	Accorde l'autorisation de répertorier les paramètres de journalisation d'accès utilisateur	Lecture			
ListUserSettings	Accorde l'autorisation de répertorier les paramètres utilisateur	Lecture			
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une ressource	Balisage	browserSettings		
			dataProtectionSettings		
			identityProvider		
			ipAccessSettings		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			networkSettings		
			portal		
			sessionLogger		
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Identification	browserSettings		
			dataProtectionSettings		
			identityProvider		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			ipAccessSettings		
			networkSettings		
			portal		
			sessionLogger		
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys	
UpdateBrowserSettings	Accorde l'autorisation de mettre à jour les paramètres de navigateur	Écrire	browserSettings*		
UpdateDataProtectionSettings	Autorise la mise à jour des paramètres de protection des données	Écrire	dataProtectionSettings*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateIdentityProvider	Accorde l'autorisation de mettre à jour un fournisseur d'identité	Écrire	identityProvider*		
			portal*		
UpdateIpAccessSettings	Accorde l'autorisation de mettre à jour des paramètres d'accès IP.	Écrire	ipAccessSettings*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateNetworkSettings	Accorde l'autorisation de mettre à jour les paramètres réseau	Écrire	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
UpdatePortal	Accorde l'autorisation de mettre à jour les portails web	Écrire	portal*		
UpdateSessionLogger	Autorise la mise à jour de l'enregistreur de session	Écrire	sessionLogger*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateTrustStore	Accorde l'autorisation de mettre à jour les magasins d'approbations	Écrire	trustStore*		
UpdateUserAccessLoggingSettings	Accorde l'autorisation de mettre à jour les paramètres de journalisation d'accès utilisateur	Écrire	userAccessLoggingSettings*		kinesis:PutRecord kinesis:PutRecords
UpdateUserSettings	Accorde l'autorisation de mettre à jour les paramètres utilisateur	Écrire	userSettings*		

Types de ressources définis par Amazon WorkSpaces Secure Browser

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
browserSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:browserSettings/${BrowserSettingsId}`	aws:ResourceTag/${TagKey}

Types de ressources	ARN	Clés de condition
identityProvider	arn:${Partition}:workspaces-web:${Region}:${Account}:identityProvider/${PortalId}/${IdentityProviderId}	aws:ResourceTag/${TagKey}
networkSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:networkSettings/${NetworkSettingsId}	aws:ResourceTag/${TagKey}
portal	arn:${Partition}:workspaces-web:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
trustStore	arn:${Partition}:workspaces-web:${Region}:${Account}:trustStore/${TrustStoreId}	aws:ResourceTag/${TagKey}
userSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userSettings/${UserSettingsId}	aws:ResourceTag/${TagKey}
userAccessLoggingSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userAccessLoggingSettings/${UserAccessLoggingSettingsId}	aws:ResourceTag/${TagKey}
ipAccessSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:ipAccessSettings/${IpAccessSettingsId}	aws:ResourceTag/${TagKey}
dataProtectionSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:dataProtectionSettings/${DataProtectionSettingsId}	aws:ResourceTag/${TagKey}
sessionLogger	arn:${Partition}:workspaces-web:${Region}:${Account}:sessionLogger/${SessionLoggerId}	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client (préfixe de service :`thinclient`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par Amazon WorkSpaces Thin Client
- Types de ressources définis par Amazon WorkSpaces Thin Client
- Clés de condition pour Amazon WorkSpaces Thin Client

Actions définies par Amazon WorkSpaces Thin Client

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
CreateEnvironment	Octroie l'autorisation de créer des environnements.	Écrire		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	appstream:DescribeStacks iam:CreateServiceLinkedRole workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:Describ

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
					eWorkspaceDirectories
DeleteDevice	Octroie l'autorisation de supprimer des appareils.	Écrire	device*		
				aws:ResourceTag/${TagKey}	
DeleteEnvironment	Octroie l'autorisation de supprimer des environnements.	Écrire	environment*		
				aws:ResourceTag/${TagKey}	
DeregisterDevice	Octroie l'autorisation d'annuler l'enregistrement d'appareils.	Écrire	device*		
				aws:ResourceTag/${TagKey}	
GetDevice	Accorde l'autorisation d'obtenir des appareils	Lecture	device*		
				aws:ResourceTag/${TagKey}	
GetDeviceDetails [autorisation uniquement]	Octroie l'autorisation d'obtenir les informations relatives à des appareils.	Lecture	device*		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:ResourceTag/${TagKey}	
GetEnvironment	Octroie l'autorisation d'obtenir les informations relatives à des environnements.	Lecture	environment*		
				aws:ResourceTag/${TagKey}	
GetSoftwareSet	Octroie l'autorisation d'obtenir les informations relatives à des ensembles de logiciels.	Lecture	softwareset*		
				aws:ResourceTag/${TagKey}	
ListDeviceSessions [autorisation uniquement]	Octroie l'autorisation de répertorier les sessions d'appareils.	List	device*		
				aws:ResourceTag/${TagKey}	
ListDevices	Accorde l'autorisation de répertorier les périphériques	List			
ListEnvironments	Accorde l'autorisation de répertorier les environnements	List			
ListSoftwareSets	Octroie l'autorisation de répertorier les ensembles de logiciels.	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises d'une ressource.	List	device		
			environment		
			softwareset		
				aws:ResourceTag/${TagKey}	
TagResource	Accorde l'autorisation d'ajouter une ou plusieurs balises à une ressource	Balisage	device		
			environment		
			softwareset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Accorde l'autorisation de supprimer une ou plusieurs balises d'une ressource	Identification	device		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
			environment		
			softwareset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateDevice	Octroie l'autorisation de mettre à jour les appareils.	Écrire	device*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
UpdateEnvironment	Octroie l'autorisation de mettre à jour des environnements.	Écrire	environment*		appstream:DescribeStacks workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories
				aws:ResourceTag/${TagKey}	
UpdateSoftwareSet	Octroie l'autorisation de mettre à jour les ensembles de logiciels.	Écrire	softwareset*		
				aws:ResourceTag/${TagKey}	

Types de ressources définis par Amazon WorkSpaces Thin Client

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
environment	`arn:${Partition}:thinclient:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:thinclient:${Region}:${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}
softwareset	`arn:${Partition}:thinclient:${Region}:${Account}:softwareset/${SoftwareSetId}`	aws:ResourceTag/${TagKey}

Clés de condition pour Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne

Clés de condition	Description	Type
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString

Actions, ressources et clés de condition pour AWS X-Ray

AWS X-Ray (préfixe de service :`xray`) fournit les ressources, actions et clés de contexte de condition spécifiques aux services suivantes à utiliser dans les politiques d'autorisation IAM.

Références :

- Découvrez comment configurer ce service.
- Affichez la liste des opérations d'API disponibles pour ce service.
- Découvrez comment protéger ce service et ses ressources avec les stratégies d'autorisation IAM.

Rubriques

- Actions définies par AWS X-Ray
- Types de ressources définis par AWS X-Ray
- Clés de condition pour AWS X-Ray

Actions définies par AWS X-Ray

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API ou à la commande CLI portant le même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations. D'autres opérations, quant à elles, requièrent plusieurs actions différentes.

La colonne Niveau d'accès du tableau Actions décrit la manière dont l'action est classée (liste, lecture, gestion des autorisations ou balisage). Cette classification peut vous aider à comprendre le

niveau d'accès accordé par une action utilisée dans une politique. Pour plus d'informations sur les niveaux d'accès, consultez la section Niveaux d'accès dans les résumés des politiques.

La colonne Types de ressources indique si chaque action prend en charge les autorisations au niveau des ressources. S'il n'y a pas de valeur pour cette colonne, vous devez indiquer toutes les ressources (« * ») dans l'élément `Resource` de votre déclaration de politique. Si la colonne inclut un type de ressource, vous pouvez indiquer un ARN de ce type dans une déclaration avec cette action. Si l'action comporte une ou plusieurs ressources requises, l'appelant doit être autorisé à utiliser l'action avec ces ressources. Les ressources requises sont indiquées dans le tableau par un astérisque (*). Si vous limitez l'accès aux ressources avec l'`Resource`élément dans une politique IAM, vous devez inclure un ARN ou un modèle pour chaque type de ressource requis. Certaines actions prennent en charge plusieurs types de ressources. Si le type de ressource est facultatif (non indiqué comme obligatoire), vous pouvez choisir d'utiliser l'un, mais pas l'autre.

La colonne Clés de condition inclut des clés que vous pouvez spécifier dans l'élément `Condition` d'une déclaration de politique. Pour plus d'informations sur les clés de condition associées aux ressources du service, consultez la colonne Clés de condition du tableau des types de ressources.

La colonne Actions dépendantes du tableau Actions indique les autorisations supplémentaires qui peuvent être nécessaires pour lancer une action avec succès. Ces autorisations peuvent être nécessaires en plus de l'autorisation pour l'action elle-même. Lorsqu'une action spécifie des actions dépendantes, ces dépendances peuvent s'appliquer à des ressources supplémentaires définies pour cette action, et pas uniquement à la première ressource répertoriée dans le tableau.

> **Note**
>
> Les clés de condition des ressources sont répertoriées dans le tableau Types de ressources. Vous pouvez trouver un lien vers le type de ressource qui s'applique à une action dans la colonne Types de ressources (* obligatoire) du tableau Actions. Le type de ressource indiqué dans le tableau Types de ressources inclut la colonne Clés de condition, qui contient les clés de condition de ressource qui s'appliquent à une action dans le tableau Actions.

Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Actions.

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
BatchGetTraceSummaryById [autorisation uniquement]	Accorde l'autorisation de récupérer des métadonnées pour une liste des suivis spécifiés par ID	Lecture			
BatchGetTraces	Accorde l'autorisation de récupérer une liste des suivis spécifiés par ID. Chaque suivi est un ensemble de documents de segment provenant d'une seule demande. GetTraceSummaries À utiliser pour obtenir une liste de traces IDs	List			
CancelTraceRetrieval	Accorde l'autorisation d'annuler une tâche de récupération de traces en cours initiée StartTraceRetrieval à l'aide du RetrievalToken Une annulation réussie renverra une réponse HTTP 200	Lecture			
CreateGroup	Accorde l'autorisation de créer une ressource de groupe avec un nom et une expression de filtre.	Écriture	group*		
				aws:RequestTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
				aws:TagKeys	
CreateSamplingRule	Accorde l'autorisation de créer une règle permettant de contrôler le comportement d'échantillonnage pour les applications instrumentées.	Écriture	sampling-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	Accorde l'autorisation de supprimer une ressource de groupe.	Écrire	group*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Accorde l'autorisation de supprimer des politiques de ressource	Écrire		xray:ResourcePolicyName	
DeleteSamplingRule	Accorde l'autorisation de supprimer une règle d'échantillonnage.	Écrire	sampling-rule*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetDistinctTraceGraphs [autorisation uniquement]	Accorde l'autorisation de récupérer des graphes de service distincts pour une ou plusieurs traces spécifiques IDs	Lecture			
GetEncryptionConfig	Accorde l'autorisation de récupérer la configuration de chiffrement actuelle pour les données X-Ray.	Lecture			
GetGroup	Accorde l'autorisation de récupérer les détails des ressources de groupe.	Lecture	group*		
				aws:ResourceTag/${TagKey}	
GetGroups	Accorde l'autorisation de récupérer tous les détails du groupe actif.	Lecture			
GetIndexingRules	Accorde l'autorisation de récupérer toutes les règles d'indexation. Les règles d'indexation sont utilisées pour déterminer le taux d'échantillonnage côté serveur pour les spans ingérés via la destination et indexés par X-Ray CloudWatchLogs	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetInsight	Accorde l'autorisation de récupérer les détails d'une information spécifique.	Lecture			
GetInsightEvents	Accorde l'autorisation de récupérer les événements d'une information spécifique.	Lecture			
GetInsightImpactGraph	Accorde l'autorisation de récupérer la partie du graphe de service qui est affectée pour une information spécifique.	Lecture			
GetInsightSummaries	Accorde l'autorisation de récupérer le résumé de toutes les informations pour un groupe et une plage de temps à l'aide de filtres facultatifs.	Lecture			
GetRetrievedTracesGraph	Accorde l'autorisation de récupérer un graphe de service pour les traces en fonction de ce qui est spécifié dans le groupe RetrievalToken de CloudWatch journaux Transaction Search	Lecture			
GetSamplingRules	Accorde l'autorisation de récupérer toutes les règles d'échantillonnage.	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetSamplingStatisticSummaries	Accorde l'autorisation de récupérer des informations sur les résultats d'échantillonnage récents pour toutes les règles d'échantillonnage.	Lecture			
GetSamplingTargets	Accorde l'autorisation de demander un quota d'échantillonnage pour les règles que le service utilise pour échantillonner les demandes.	Lecture			
GetServiceGraph	Accorde l'autorisation de récupérer un document qui décrit les services qui traitent les demandes entrantes et les services en aval qu'ils appellent comme résultat.	Lecture			
GetTimeSeriesServiceStatistics	Accorde l'autorisation de récupérer une agrégation des statistiques de service définies par une plage de temps spécifique mises en compartiments dans des intervalles de temps.	Lecture			
GetTraceGraph	Accorde l'autorisation de récupérer un graphe de service pour une ou plusieurs traces spécifiques IDs	Lecture			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
GetTraceSegmentDestination	Accorde l'autorisation de récupérer la destination actuelle des données envoyées à une PutTraceSegments OpenTelemetry API	Lecture			
GetTraceSummaries	Accorde l'autorisation de récupérer les métadonnées des traces IDs et les rend disponibles pendant une période spécifiée à l'aide d'un filtre facultatif. Pour obtenir les traces complètes, transmettez-les IDs à BatchGetTraces	Lecture			
Link [autorisation uniquement]	Accorde l'autorisation de partager des ressources X-Ray avec un compte de surveillance	Écrire			
ListResourcePolicies	Accorde l'autorisation de répertorier les politiques de ressource	List			
ListRetrievedTraces	Accorde l'autorisation de récupérer une liste de traces pour une donnée Retrieval Token à partir du groupe de CloudWatch journaux Transaction Search	List			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
ListTagsForResource	Accorde l'autorisation de répertorier les balises pour une ressource X-Ray.	Liste	group		
			sampling-rule		
PutEncryptionConfig	Accorde l'autorisation de mettre à jour la configuration de chiffrement pour les données X-Ray.	Gestion des autorisations			
PutResourcePolicy	Accorde l'autorisation de créer ou de mettre à jour des politiques de ressource	Écrire		xray:ResourcePolicyName	
PutSpans	Autorise le téléchargement de OpenTelemetry spans vers X-Ray AWS	Écrire		logs:LogGeneratingResourceArns	
PutSpansForIndexing [autorisation uniquement]	Autorise le téléchargement de spans vers AWS X-Ray pour qu'ils soient indexés	Écrire			
PutTelemetryRecords	Autorise l'envoi de la télémétrie du démon AWS X-Ray au service	Écrire			

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
PutTraceSegments	Accorde l'autorisation de télécharger des documents segmentés sur AWS X-Ray. Le kit SDK X-Ray génère des documents de segment et les envoie au démon X-Ray, qui effectue un chargement par lots.	Écrire		logs:LogGeneratingResourceArns	
StartTraceRetrieval	Accorde l'autorisation de lancer un processus de récupération de traces en utilisant la plage de temps spécifiée et pour la trace donnée dans IDs le groupe de CloudWatch journaux Transaction Search	Lecture			
TagResource	Accorde l'autorisation d'ajouter des balises à une ressource X-Ray.	Balisage	group		
			sampling-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource		Balisage	group		

Actions	Description	Niveau d'accès	Types de ressources (*obligatoire)	Clés de condition	Actions dépendantes
	Accorde l'autorisation de supprimer les balises d'une ressource X-Ray.		sampling-rule		
				aws:TagKeys	
UpdateGroup	Accorde l'autorisation de mettre à jour une ressource de groupe.	Écrire	group*		
				aws:ResourceTag/${TagKey}	
UpdateIndexingRule	Accorde l'autorisation de modifier la configuration d'une règle d'indexation	Écrire			
UpdateSamplingRule	Accorde l'autorisation de modifier la configuration d'une règle d'échantillonnage.	Écrire	sampling-rule*		
				aws:ResourceTag/${TagKey}	
UpdateTraceSegmentDestination	Accorde l'autorisation de modifier la destination des données envoyées à une PutTraceSegments OpenTelemetry API	Écrire		xray:TraceSegmentDestination	

Types de ressources définis par AWS X-Ray

Ce service définit les types de ressources suivants, qui peuvent être utilisés dans l' `Resource` élément des déclarations de politique d'autorisation IAM. Chaque action du tableau Actions identifie les types de ressources pouvant être spécifiés avec cette action. Un type de ressource peut également définir les clés de condition que vous pouvez inclure dans une politique. Ces clés sont affichées dans la dernière colonne du tableau. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Types de ressources.

Types de ressources	ARN	Clés de condition
group	`arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}`	aws:ResourceTag/${TagKey}
sampling-rule	`arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}`	aws:ResourceTag/${TagKey}

Clés de condition pour AWS X-Ray

AWS X-Ray définit les clés de condition suivantes qui peuvent être utilisées dans l'`Condition`élément d'une politique IAM. Vous pouvez utiliser ces clés pour affiner les conditions d'application de la déclaration de politique. Pour plus de détails sur les colonnes du tableau suivant, veuillez consulter le tableau Clés de condition.

Pour afficher les clés de condition globales disponibles pour tous les services, consultez la section Clés contextuelles de condition AWS globales.

Clés de condition	Description	Type
aws:RequestTag/${TagKey}	Filtre l'accès en fonction des identifications transmises dans la demande	Chaîne
aws:ResourceTag/${TagKey}	Filtre l'accès en fonction des identifications associées à la ressource	Chaîne

Clés de condition	Description	Type
aws:TagKeys	Filtre l'accès en fonction des clés d'identification qui sont transmises dans la demande	ArrayOfString
logs:LogGenerating ResourceArns	Filtre l'accès par LogGeneratingResourceArn requête	ArrayOfARN
xray:ResourcePolicyName	Filtre l'accès par PolicyName requête	String
xray:TraceSegmentDestination	Filtre l'accès par TraceSegmentDestination type dans la demande	String

Ressources connexes

Pour obtenir des informations connexes contenues dans le Guide de l'utilisateur IAM, consultez les ressources suivantes :

- Didacticiel : Créer et attacher votre première stratégie gérée par le client
- AWS services qui fonctionnent avec IAM
- Logique d’évaluation de stratégies

Service AWS Informations simplifiées pour un accès programmatique

AWS fournit des informations de référence de service au format JSON afin de rationaliser l'automatisation des flux de travail de gestion des politiques. Grâce aux informations de référence du service, vous pouvez accéder aux opérations, actions, ressources et clés de condition disponibles Services AWS à partir de fichiers lisibles par machine. Les informations de référence du service incluent des métadonnées autres que les détails d'autorisation, notamment les informations sur les dernières actions IAM consultées et les données de génération de politiques IAM Access Analyzer.

Les administrateurs de sécurité peuvent établir des garde-fous et les développeurs peuvent garantir un accès approprié aux applications en identifiant les actions, les ressources et les clés de condition disponibles pour chacune d'entre elles. Service AWS AWS fournit des informations de référence sur les services Services AWS pour vous permettre d'intégrer les métadonnées dans vos flux de travail de gestion des politiques.

- Pour un inventaire des actions, des ressources et des clés de condition à utiliser dans les politiques IAM, consultez la page de référence des autorisations de service pour le Service AWS. Les actions, les ressources et les clés de condition pour les services qui partagent un préfixe de service peuvent être réparties sur plusieurs pages dans la référence d'autorisation de service.
- Pour obtenir la liste des actions pour lesquelles les informations du dernier accès à l'action IAM sont affichées, consultez la section Actions Services AWS et services d'information auxquels vous avez accédé pour la dernière fois lors de l'action IAM dans le Guide de l'utilisateur IAM.
- Pour obtenir une liste Services AWS des actions pour lesquelles IAM Access Analyzer génère des politiques avec des informations au niveau des actions, voir les services de génération de politiques IAM Access Analyzer dans le guide de l'utilisateur d'IAM.

Le contenu présenté dans la référence d'autorisation de service peut être présenté différemment ou contenir des métadonnées différentes. Pour de plus amples informations, veuillez consulter Définitions de champs supplémentaires.

Les informations de référence du service fournissent également des métadonnées sur les opérations, y compris des informations sur les actions autorisées et les noms des méthodes SDKs.

Un contexte supplémentaire concernant la valeur des clés de condition peut être disponible pour aider à définir la portée des autorisations. Par exemple, la valeur de `iam:PassedToService` peut apparaître lorsque l'action `iam:PassRole` est autorisée par une opération.

Ce mappage opération-action n'est pas pris en charge pour tous les services. Les services qui ne prennent pas encore en charge ce mappage omettront cette AuthorizedAction propriété. En outre, les informations relatives aux actions autorisées relatives aux opérations n'incluent pas les autorisations qui peuvent être requises pour les opérations effectuées en votre nom dans le cadre de sessions d'accès direct.

> **Note**
>
> Les modifications apportées aux informations de référence du service peuvent prendre jusqu'à 24 heures pour être prises en compte dans la liste des métadonnées du service.

Accès aux informations Service AWS de référence

1. Accédez aux informations de référence du service Services AWS pour accéder à la liste des informations de référence disponibles.

   Il existe deux principaux points d'entrée :

   http://servicereference.us-east-1.amazonaws.com/ affiche une liste Services AWS des informations de référence disponibles.

   L'exemple suivant montre une liste partielle des services et URLs leurs informations de référence respectives :

   ```
   [
       {
           "service": "s3",
           "url": "https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json"
       },
       {
           "service": "dynamodb",
           "url": "https://servicereference.us-east-1.amazonaws.com/v1/dynamodb/
   dynamodb.json"
       },
       …
   ```

```
]
```

https://servicereference.us-east-1.amazonaws.com/v1/mapping.json affiche un mappage entre les services du SDK et l'emplacement dans la référence de service sous lequel les informations se trouvent.

L'exemple suivant montre une liste partielle de mappages :

```
{
  "SDK" : {
    "Python" : {
      "Boto3" : {
        "accessanalyzer" : {
          "service" : "access-analyzer",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/access-
analyzer/access-analyzer.json"
        },
        "account" : {
          "service" : "account",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/account/
account.json"
        },
        "amp" : {
          "service" : "aps",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/aps/
aps.json"
        },
        ...
      }
    }
  }
}
```

2. Choisissez un service et accédez à la page d'informations du service dans le `url` champ correspondant pour afficher la liste des actions, des ressources et des clés de condition associées au service.

   L'exemple suivant montre une liste partielle d'informations de référence de service pour Amazon S3 :

```
{
    "Name": "s3",
```

```
    "Actions": [
        {
            "Name": "GetObject",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ExistingObjectTag/key",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:if-match",
                "s3:if-none-match",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
            "Properties" : {
                    "IsList" : false,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "object"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        {
            "Name": "ListBucket",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ResourceAccount",
```

```
                "s3:TlsVersion",
                "s3:authType",
                "s3:delimiter",
                "s3:max-keys",
                "s3:prefix",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : true,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "bucket"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        ...
    ],
    "ConditionKeys": [
        {
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
```

```
    "Operations": [
        {
            "Name" : "GetObject",
            "AuthorizedActions" : [
                {
                    "Name" : "GetObject",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObject",
                    "Service" : "s3-object-lambda"
                }, {
                    "Name" : "GetObjectLegalHold",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectRetention",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectTagging",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectVersion",
                    "Service" : "s3"
                }
            ],
            "SDK" : [
                {
                    "Name" : "s3",
                    "Method" : "get_object",
                    "Package" : "Boto3"
                }
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
            ]
        },
        {
            "Name": "bucket",
```

```
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
    "Version": "v1.4"
}
```

3. Téléchargez le fichier JSON à partir de l'URL du service pour l'utiliser dans vos flux de travail de création de politiques.

Glossaire

- Fonctionnement : une API qui peut être appelée, généralement par le biais d'un SDK
- Action : autorisation autorisée lors de l'exécution d'une opération

Définitions de champs supplémentaires

Les propriétés d'action fournissent des métadonnées supplémentaires sur les actions de service afin de les classer en fonction de leur étendue d'autorisation. Ces propriétés se trouvent sous le `Annotations` champ pour chaque action. Les métadonnées se composent de quatre valeurs booléennes :

- `IsList`— Permet de découvrir et de répertorier les ressources, y compris les métadonnées de base, sans accéder au contenu des ressources.

  Exemple — Cette propriété `true` concerne l'`ListBucket`action Amazon S3, qui permet aux utilisateurs de consulter les listes de compartiments sans accéder aux objets eux-mêmes.
- `IsPermissionManagement`— Fournit des autorisations pour modifier les autorisations IAM ou les informations d'identification d'accès.

  Exemple — Cette propriété concerne la plupart `true` des AWS Organizations actions et IAM, ainsi que des actions Amazon S3 telles que `PutBucketPolicy` et`DeleteBucketPolicy`.
- `IsTaggingOnly`— Fournit des autorisations uniquement pour modifier les balises.

Exemple — Cette propriété est `true` destinée aux actions `TagRole` IAM`UntagRole`, alors que cette propriété l'est `false` `CreateRole` car elle fournit des autorisations plus étendues que le balisage.

- `IsWrite`— Fournit des autorisations pour modifier les ressources, ce qui peut inclure des modifications de balises.

  Exemple — Cette propriété concerne `true` les actions Amazon S3 `CreateBucket`, `DeleteBucket`, et `PutObject` étant donné qu'elles autorisent la modification des ressources.

> **Note**
>
> Ces propriétés ne s'excluent pas mutuellement. Une action peut avoir plusieurs propriétés définies sur`true`.
> Il est également possible que toutes les propriétés le soient`false`, comme en témoigne l'`GetObject`action d'Amazon S3. Cela indique que l'action accorde uniquement des autorisations de lecture sur un objet.

Ces propriétés peuvent être utilisées pour générer des informations pour les services. L'exemple suivant montre quelles autorisations avec le `s3` préfixe autorisent la mutation des ressources :

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsWrite == true) | .Name'

"AssociateAccessGrantsIdentityCenter"
"BypassGovernanceRetention"
"CreateAccessGrant"
"CreateAccessGrantsInstance"
"CreateAccessGrantsLocation"
...
```

L'exemple suivant montre les clés de condition d'action avec le `lambda` préfixe que vous pouvez utiliser pour limiter l'accès aux actions de gestion des autorisations :

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/lambda/lambda.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsPermissionManagement == true) |
 {Name: .Name, ActionConditionKeys: (.ActionConditionKeys // [])}'
```

```
{
   "Name": "AddLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "AddPermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
{
    "Name": "DisableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "EnableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "RemoveLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "RemovePermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
```

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.